

1 David M. Given (State Bar No. 142375)
2 Nicholas A. Carlin (State Bar No. 112532)
3 PHILLIPS, ERLEWINE & GIVEN LLP
4 50 California Street, 32nd Floor
5 San Francisco, CA 94111
6 Tel: 415-398-0900
7 Fax: 415-398-0911
8 Email: dmg@phillaw.com
9 nac@phillaw.com

6 James M. Wagstaffe (State Bar No. 95535)
7 Michael Ng (State Bar No. 237915)
8 Michael von Loewenfeldt (State Bar No. 178665)
9 Ivo Labar (State Bar No. 203492)
10 KERR & WAGSTAFFE LLP
11 100 Spear Street, 18th Floor
12 San Francisco, CA 94105-1528
13 Telephone: (415) 371-8500
14 Fax: (415) 371-0500
15 Email: wagstaffe@kerrwagstaffe.com
16 mng@kerrwagstaffe.com
17 mvl@kerrwagstaffe.com
18 labar@kerrwagstaffe.com

13 Interim Lead Counsel for Plaintiffs
14 [ADDITIONAL COUNSEL LISTED BELOW]

15 **UNITED STATES DISTRICT COURT**
16 **NORTHERN DISTRICT OF CALIFORNIA**

17 IN RE:

18 APPLE IDEVICE ADDRESS BOOK
19 LITIGATION

Case No. 13-cv-00453-JST

CLASS ACTION

**OPPERMAN PLAINTIFFS’ OPPOSITION TO
DEFENDANT APPLE, INC.’S MOTION TO
DISMISS CONSOLIDATED AMENDED
CLASS ACTION COMPLAINT;
MEMORANDUM OF POINTS AND
AUTHORITIES IN SUPPORT THEREOF**

Hernandez v. Path, Inc., No. 12-cv-1515-JST
Pirozzi v. Apple, Inc., No. 12-cv-1529-JST
Gutierrez v. Instagram, Inc., No. 12-cv-6550-JST
Espitia v. Hipster, Inc., No. 4:13-cv-432-JST
(collectively, the “Related Actions”)

Date: January 22, 2014
Time: 9:30 A.M.
Courtroom: 9, 19th Floor

TABLE OF CONTENTS

	<i>Page</i>
1	
2	I. INTRODUCTION 1
3	II. RELEVANT FACTS 3
4	III. ARGUMENT 9
5	A. Section 230 of the CDA Does Not Bar Plaintiffs’ Claims Against Apple 9
6	1. The Motion to Dismiss Stage is Not a Proper Time to Resolve Whether
7	the CDA Applies..... 9
8	2. Section 230(c)(1) Provides No Defense to Apple Because Plaintiffs’
9	Claims Arise From Apple’s Conduct, Not From Passive Transmission of
10	Third Party Content..... 11
11	3. Section 230(c)(2) Provides No Defense to Apple Because Apple is not
12	Being Sued for Blocking Content 15
13	B. This Court Clearly Has Jurisdiction Over This Action Because Plaintiffs Have
14	Standing To Pursue Their Claims Against Apple..... 16
15	1. Apple's Motion Misapplies the Standard for 12(b)(1) 18
16	2. Plaintiffs’ Injunctive and Statutory Claims Create Standing 19
17	3. Plaintiffs Have Standing to Bring the Non-Statutory Claims 20
18	4. Non-California Plaintiffs Have Standing to Bring Claims Based on
19	California Statutes..... 25
20	C. Plaintiffs’ Misrepresentation Claims Against Apple Are Properly Pled 27
21	1. The Court Has Already Upheld These Claims 27
22	2. Plaintiffs Have Met the Requirements of Rule 9(b) 28
23	3. The CAC Details Apple’s False and Misleading Statements 30
24	4. Apple’s Arguments Are Unavailing 34
25	5. Class Claims Based on Misrepresentations the Class Representatives Did
26	Not See May Be Maintained..... 36
27	6. Apple’s Material Omissions Give Rise to Liability..... 36
28	D. Plaintiffs’ Other Claims Are All Properly Pled 41
	a) California Computer Crime Law, Cal. Penal Code § 502 41
	b) Conversion..... 42

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

c) Trespass to Chattels	43
d) Strict Products Liability	44
e) Negligence	47
f) Aiding and Abetting	49

IV. CONCLUSION.....	50
---------------------	----

TABLE OF AUTHORITIES

	<i>Pages</i>
<u>Cases</u>	
1 <u>Arakaki v. Lingle,</u>	
2 477 F.3d 1048 (9th Cir. 2007)	17
3 <u>Astiana v. Ben & Jerry’s Homemade, Inc.,</u>	
4 2011 WL 2111796 (N.D. Cal. May 26, 2011)	29
5 <u>Atl. Recording Corp. v. Project Playlist, Inc.,</u>	
6 603 F. Supp. 2d 690 (S.D.N.Y. 2009).....	11
7 <u>Augustine v. United States,</u>	
8 704 F.2d 1074 (9th Cir. 1983)	18
9 <u>Baba v. Hewlett-Packard Co.,</u>	
10 2010 WL 2486353 (N.D. Cal. June 16, 2010)	35, 39, 40
11 <u>Bardin v. Daimlerchrysler Corp.,</u>	
12 136 Cal. App. 4th 1255 (2006)	39
13 <u>Barnes v. Yahoo!, Inc.,</u>	
14 570 F.3d 1096 (9th Cir. 2009)	9
15 <u>Barter v. Lull Engineering,</u>	
16 20 Cal. 3d 413 (1978)	45
17 <u>Bates v. United Parcel Serv., Inc.,</u>	
18 511 F.3d 974 (9th Cir. 2007)	19
19 <u>Batzel v. Smith,</u>	
20 333 F.3d 1018 (9th Cir. 2003)	12, 16
21 <u>Berly v. D & L Sec. Svcs. and Investigations, Inc.,</u>	
22 876 S.W.2d 179 (Tex. 1994).....	49
23 <u>Bilodeau v. McAfee, Inc.,</u>	
24 2013 WL 3200658 (N.D. Cal. June 24, 2013)	24
25 <u>Birdsong v. Apple,</u>	
26 590 F.3d 955 (9th Cir. 2009)	41
27 <u>Bolin v. Tenneco Oil Co.,</u>	
28 373 S.W.2d 350 (Tex. 1963).....	47
<u>Brazil v. Dole Food Co.,</u>	
935 F. Supp. 2d 947 (N.D. Cal. 2013)	24
<u>Bruno v. Eckhart Corp.,</u>	
280 F.R.D. 540 (C.D. Cal. Mar. 6, 2012)	27
<u>Bruno v. Outen Research Inst., LLC,</u>	
280 F.R.D. 524 (C.D. Cal. 2011)	36
<u>Bruton v. Gerber Prods. Co.,</u>	
2013 WL 4833413 (N.D. Cal. Sept. 6, 2013)	34

1 Carafano v. Metrosplsh.com, Inc.,
339 F.3d 1119 (9th Cir. 2003) 9, 12

2 Cardenas v. NBTY, Inc.,
870 F. Supp. 2d 984 (E.D. Cal. 2012)..... 36

3

4 Catholic League for Religious and Civil Rights v. City & Cnty. of S.F.,
624 F.3d 1043 (9th Cir.2010) 17

5 Cattie v. Walmart Stores, Inc.,
504 F. Supp. 2d 939 (S.D. Cal. 2007)..... 22

6

7 Chacanaca v. Quaker Oats Co.,
752 F. Supp. 2d 1111 (N.D. Cal. 2010) 29

8 Clancy v. The Bromley Tea Co.,
2013 WL 4081632 (N.D. Cal., Aug. 9, 2013) 22, 29, 36

9

10 Clothesrigger, Inc. v. GTE Corp.,
191 Cal. App. 3d 605 (1987) 25

11 Cole v. General Motors,
484 F.3d 717 (5th Cir. 2007) 24

12

13 Collins v. eMachines, Inc.,
202 Cal. App. 4th 249 (2011) 38, 39

14 Cooper v. Pickett,
137 F.3d 616 (9th Cir. 1998) 28

15

16 Daugherty v. American Honda Motor Co., Inc.,
144 Cal. App. 4th 824 (2006) 39

17 Delacruz v. Cytosport, Inc.,
2012 WL 1215243 (N.D. Cal. Apr. 11, 2012) 24, 34

18

19 Doe v. MySpace, Inc.,
474 F. Supp. 2d. 843 (W.D. Tex. 2007)..... 16

20 Doe v. MySpace, Inc.,
528 F.3d 413 (5th Cir. 2008) 16

21

22 Donohue v. Apple, Inc.,
2012 WL 1657119 (N.D. Cal. May 10, 2012) 20

23 Donohue v. Apple, Inc.,
871 F. Supp. 2d 913 (N.D. Cal. 2012) 27, 40

24

25 Durell v. Sharp Healthcare,
183 Cal. App. 4th 1350 (2010) 34

26 Edwards v. First American Corp.,
610 F.3d 514 (9th Cir. 2010) 19

27

28 El Chico Corp. v. Poole,
732 S.W.2d 306 (Tex. 1987)..... 47

1 Equity Lifestyle Props., Inc. v. County of San Luis Obispo,
548 F.3d 1184 (9th Cir. 2008) 17

2 Evans v. Hewlett-Packard Co.,
2013 WL 5594717 (N.D. Cal. Oct. 10, 2013)..... 10

3

4 Fabozzi v. StubHub, Inc.,
2012 WL 506330 (N.D. Cal. Feb. 15, 2012) 40

5 Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC,
521 F.3d 1157 (9th Cir. 2008) 10, 11, 12, 13

6

7 Falk v. General Motors Corp.,
496 F. Supp. 2d 1088 (N.D. Cal. 2007) 38

8 Fid. Union Trust Co. v. Field,
311 U.S. 169 (1940)..... 27

9

10 Fraley v. Facebook, Inc.,
830 F. Supp. 2d 785 (N.D. Cal. 2011) 12, 14, 17

11 Garcia v. Sony Computer Entm't Am., LLC,
859 F. Supp. 2d 1056 (N.D. Cal. 2012) 34

12

13 Gitson v. Trader Joe's Co.,
2013 WL 5513711 (N.D. Cal. Oct. 4, 2013)..... 34

14 Goodman v. HTC America, Inc.,
2012 WL 2412070 (W.D. Wash. Jun. 26, 2012) 20, 28

15

16 Gould Electronics, Inc. v. United States,
220 F.3d 169 (3rd Cir. 2000) 18

17 Haskins v. Symantec Corp.,
2013 WL 4516179 (N.D. Cal. Aug. 23, 2013) 17, 22

18

19 Hepting v. AT&T Corp,
439 F. Supp. 2d 974 (N.D. Cal. 2006) 21

20 Hodgers-Durgin v. de la Vina,
199 F.3d 1037 (9th Cir. 1999) 19

21

22 Holomaxx Tech.s v. Microsoft Corp.,
783 F. Supp. 2d 1097 (N.D. Cal. 2011) 10, 16

23 Horton v. Jack,
126 Cal. 521 (1899) 42

24

25 Hunt v. Baldwin,
68 S.W.3d 117 (Tex. 2001)..... 42

26 In re Apple & AT & T iPad Unlimited Data Plan Litig.
802 F. Supp. 2d 1070 (N.D. Cal. 2011) 26

27

28 In re Google Android Consumer Privacy Litig.,
2013 WL 1283236 (N.D. Cal. Mar. 26, 2013)..... 35

1 In re iPhone 4S Consumer Litig.
2013 WL 3829653 (N.D. Cal. July 23, 2013)..... 26

2 In re iPhone Application Litig.
3 2011 WL 4403963 (N.D. Cal Sept. 20, 2011) 21

4 In re iPhone Application Litig.
844 F. Supp. 2d 1040 (N.D. Cal. 2012) 21, 28, 30

5 In re POM Wonderful LLC Mktg. and Sales Practices Litig.
6 2012 WL 4490860 (C.D. Cal. Sept. 28, 2012) 27

7 In re Tobacco II Cases,
46 Cal.4th 298 (2009) 28, 30

8 Intel v. Hamidi,
9 30 Cal.4th 1342 (2003) 43

10 Janda v. T-Mobile, USA, Inc.,
2009 WL 667206 (N.D. Cal. Mar. 13, 2009)..... 41

11 Joffe v. Google, Inc.,
12 729 F.3d 1262 (9th Cir. 2013) 8

13 Johnson v. American Standard, Inc.,
43 Cal 4th 56 (2008) 45

14 Kane v. Chobani, Inc.,
15 2013 WL 5289253 (N.D. Cal. Sep. 19, 2013) 35

16 Kearns v. Ford Motor Co.,
567 F.3d 1120 (9th Cir. 2009) 28

17 Keegan v. Am. Honda Motor Co., Inc.,
18 284 F.R.D. 504 (C.D. Cal. 2012) 39

19 Kerns v. United States,
585 F.3d 187 (4th Cir. 2009) 18

20 Klaxon Co. v. Stentor Elec. Mfg. Co.,
21 313 U.S. 487 (1941)..... 27

22 Koehler v. Litehouse, Inc.,
2012 WL 6217635 (N.D. Cal. Dec. 13, 2012)..... 36

23 Kosta v. Del Monte Corp.,
24 2013 WL 2147413 (N.D. Cal., May 15, 2013)..... 23

25 Kwikset v. Superior Court,
51 Cal.4th 310 (2011) 20, 24

26 Lilly v. Jamba Juice Co.,
27 2013 WL 6070503 (N.D. Cal. Nov. 18, 2013) 19

28 Lima v. Gateway, Inc.,
710 F. Supp. 2d 1000 (C.D. Cal. 2010) 29

1 LiMandri v. Judkins,
52 Cal. App. 4th 326 (1997) 38

2 LinkedIn User Privacy Litig.,
932 F. Supp. 2d 1089 (N.D. Cal. 2013) 23

3

4 Lujan v. Defenders of Wildlife,
504 U.S. 555 (1992)..... 17, 20

5 Maya v. Centex,
658 F.3d 1060 (9th Cir. 2011) 24

6

7 Mazza v. American Honda Motor Co., Inc.,
666 F.3d 581 (9th Cir. 2012) 26

8 Melendres v. Arpaio,
695 F.3d 990 (9th Cir. 2012) 19

9

10 Mirkin v. Wasserman,
5 Cal. 4th 1082 (1993) 38

11 Missouri, K & T. RR. Co. of Texas v. Wood,
66 S.W. 449 (Tex. 1902)..... 48

12

13 Morgan v. AT & T Wireless Servs., Inc.,
177 Cal. App. 4th 1235 (2009) 29

14 Nelson v. Superior Court,
144 Cal App. 4th 689 (2006). 45

15

16 Nelson v. Superior Court,
144 Cal. App. 4th 689 (2006) 45

17 Nicacio v. U.S. I.N.S.,
797 F.2d 700 (9th Cir. 1985) 19

18

19 O’Neil v. Crane,
53 Cal.4th 335 (2012) 45, 47

20 Omnibus Int’l, Inc. v. AT&T, Inc.,
111 S.W.3d 818 (Tex. 2003)..... 43

21

22 Otis Eng’g Corp. v. Clark,
668 S.W.2d 307 (Tex. 1983)..... 48

23 Overton v. Bird Brain, Inc.,
2012 WL 909295 (C.D. Cal. Mar. 15, 2012)..... 38

24

25 Perfect 10, Inc. v. Google, Inc.,
2008 WL 4217837 (C.D. Cal. 2008)..... 10

26 Peterson v. Boeing Co,
715 F.3d 276 (9th Cir. 2013) 18

27

28 Pirozzi v. Apple Inc.,
913 F. Supp. 2d 840 (N.D. Cal. 2012) 9

1 Pirozzi v. Apple, Inc.,
2013 WL 4029067 (N.D. Cal. Aug. 5, 2013) 20, 21, 27, 33

2 Presley v. Cooper,
3 284 S.W.2d 138 (1955)..... 42

4 S.R.P. ex rel. Abunabba v. United States,
676 F.3d 329 (3rd Cir. 2012) 18

5 Safe Air for Everyone v. Meyer,
6 373 F.3d 1035 (9th Cir. 2004) 18

7 Stearns v. Ticketmaster Corp.,
655 F.3d 1013 (9th Cir. 2011) 19

8 Stratton Oakmont, Inc. v. Prodigy Services Co.,
9 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995)..... 11

10 Sullivan v. Oracle Corp.,
51 Cal. 4th 1191 (2011) 25

11 Swift v. Zynga Game Network, Inc.,
12 2010 WL 4569889 (N.D. Cal. Nov. 3, 2010) 10, 12, 13

13 Tellez Cordova v Campbell-Hausfeld/Scott Felzger Co.,
129 Cal. App. 4th 577 (2004)..... 46, 47

14 Ticketmaster L.L.C. v. RMG Technologies,
15 2007 WL 2989504 (C.D. Cal. Oct. 12, 2007)..... 28

16 Tietsworth v. Sears, Roebuck & Co.,
720 F. Supp. 2d 1123 (N.D. Cal. 2010) 39

17 U.S. ex rel. Lee v. SmithKline Beecham, Inc.,
18 245 F.3d 1048 (9th Cir. 2001) 28

19 United States v. Students Challenging Regulatory Agency Procedures,
412 U.S. 669 (1973)..... 17

20 Vess v. Ciba-Geigy Corp. USA,
21 317 F.3d 1097 (9th Cir. 2003) 28

22 Vitt v. Apple Computer, Inc.,
469 Fed. Appx. 605 (9th Cir. 2012)..... 40

23 Warren v. Fox Family Worldwide, Inc.,
24 328 F.3d. 1136 (9th Cir. 2003) 18

25 Warth v. Seldin,
422 U.S. 490 (1975)..... 17, 19

26 Wershba v. Apple Computer, Inc.,
27 91 Cal. App. 4th 224 (2001) 25

28 Williamson v. Reinalt-Thomas Corp.,
2012 WL 1438812 (N.D. Cal. Apr. 25, 2012) 22

1 Wilson v. Brister,
982 S.W.2d 42 (Tex. 1998)..... 49

2 Wilson v. Hewlett-Packard Co.,
668 F.3d 1136 (9th Cir. 2012) 38

3

4 Womack v. Nissan N. Am., Inc.,
550 F. Supp. 2d 630 (E.D. Tex. 2007)..... 20

5 Zango, Inc. v. Kaspersky Lab, Inc.,
568 F.3d 1169 (9th Cir. 2009) 16

6

7 Zapata v. Ford Motor Credit Co.,
615 S.W.2d 198 (Tex. 1981)..... 43

8

9 Statutes

9 47 U.S.C. § 230..... passim

10 Cal. Penal Code § 502..... 41

11 Texas Civil Practices and Remedies Code § 82.003..... 49

12

13 Other Authorities

13 Schwarzer, et al., Cal. Prac. Guides: Fed. Civ. Pro. Before Trial,
14 ¶ 9:211 (TRG 2013)..... 18

15

16 Rules

16 Fed. R. Civ. P 56..... 18

17 Fed. R. Civ. P. 12..... 18

18 Fed. R. Civ. P. 9..... 28, 29

1 Plaintiffs Haig Arabian, Alan Beuershasen, Giuli Biondi, Lauren Carter, Steve Dean,
 2 Stephanie Dennis-Cooley, Jason Gree, Claire Hodgins, Gentry Hoffman, Rachelle King, Nirali
 3 Mandaywala, Claire Moses, Judy Paul, Maria Pirozzi, Theda Sandiford and Greg Varner
 4 (collectively, “Plaintiffs”) submit this memorandum of law in opposition of Apple Inc.’s
 5 (“Apple”) motion to dismiss their Consolidated Amended Complaint (“CAC”).

6 I. INTRODUCTION

7 The principle that appears to be guiding the Defendants in this action is the following: if a
 8 user receives a free computer-related service, he or she becomes a commodity to be sold in the
 9 new surveillance economy.

10 In this case, Apple has practically created its own market for smart phones and tablets,
 11 portable all-in-one devices that allow people to carry what used to be a desk full of equipment,
 12 and libraries full of information, in their pockets. Apple built this market in large part based on
 13 its constant public assurances that its products were secure, and that the personal data consumers
 14 choose to store on them cannot be taken without permission. Unfortunately, those assurances
 15 were false. Numerous “apps” (a shorthand popularized by Apple for “software application”)
 16 jointly developed, promoted, and sold by Apple (in concert with the other Defendants to this
 17 action) copied users’ Contacts information¹ from their iDevices and transmitted a copy of those
 18 Contacts to the developer of the app (and perhaps others beyond that).

19 Apple has repeatedly assured consumers that apps cannot access other apps and that
 20 stealing information between apps is not possible. Apple maintains near total control over the
 21 iDevices and aggressively limits what software can be installed on the iDevices both through its
 22 proprietary operating system (“iOS”) and by maintaining a single source for all apps: Apple’s
 23

24
 25
 26 ¹ The Contacts app, which comes pre-programmed by Apple on each iDevice, allows users
 27 to customize contacts information using the following fields: (1) first and last name and phonetic
 28 spelling of each; (2) nickname; (3) company, job title, and department; (4) address(es); (5) phone
 number(s); (6) email address(es); (7) instant messenger contact; (8) photo; (9) birthday; (10)
 related people; (11) homepage; (12) notes; (13) ringtone; and (14) text tone.

1 “App Store.” Yet now that it is clear that apps *do* regularly take Contact information without
2 clear, contemporaneous permission from the user, Apple seeks to avoid all responsibility.

3 Apple first argues that Section 230 of the Communications Decency Act, 47 U.S.C. § 230
4 (“CDA”) – designed to provide websites with immunity from defamation claims regarding
5 content posted on the sites by third parties – immunizes Apple from any liability for what apps
6 do. This argument was already considered and rejected by Judge Rogers in Pirozzi v. Apple Inc.,
7 12-cv-1529 (“Pirozzi I”). The Apple App Store is the polar opposite of a passive website.
8 Apple is deeply involved in and controls every aspect of an app’s development and deployment.
9 The CDA provides no safe harbor for Apple’s misconduct, and it certainly provides no immunity
10 from claims that Apple made misrepresentations about the iDevices themselves.

11 Apple next argues that Plaintiffs lack standing to pursue their claims, even though
12 Plaintiffs are indisputably suing over something that happened *to them*. Apple’s arguments
13 misunderstand Article III standing requirements, and seek to transform standing from a means of
14 assuring that suits are not brought by uninvolved strangers into an early test of the merits of a
15 case.

16 Apple also argues that even though it is headquartered in California and conducts most of
17 its relevant operations here, it cannot be sued under California law by people who live out of
18 state. Apple’s argument relies on an over-reading of an inapposite wage and hour case as well as
19 a willful blindness to the facts alleged here.

20 Next, Apple argues that it cannot be sued under various theories either for
21 misrepresentation or omission of fact because, amongst the sea of advertising Apple has
22 broadcast to the world, Apple thinks the Plaintiffs cannot point to the one specific statement that
23 they relied on (or that Plaintiffs are remembering the wrong statement). These arguments ignore
24 a host of authority recognizing that lengthy, well-broadcast advertising campaigns can create
25 misrepresentation liability.

26 Finally, Apple insists that it is not liable for various statutory or common law torts arising
27 from its conduct. As discussed below, in each instance, Apple relies on a cramped reading of
28

1 both case law and the alleged facts. Plaintiffs have pled valid theories against Apple, and are
2 entitled to engage in discovery to further seek to prove their allegations.

3 **II. RELEVANT FACTS**

4 Neither Apple nor its various iDevices (iPhone, iPad, iPod Touch) need any introduction
5 to this Court. The ubiquitous role this company and its products have taken in contemporary
6 American life is a tribute to the inventiveness of Apple's designers and, more importantly for this
7 case, the pervasiveness and effectiveness of Apple's advertising and branding campaigns.
8

9 Apple designs both the hardware component of the iDevices as well as the the iOS that
10 runs each device. (CAC ¶ 65.) The iPhone is the most popular of the three devices; however,
11 the three devices share many of the same apps. (CAC ¶¶ 66, 69.) The iPhone combines a
12 mobile phone, an iPod (or digital music and media player), and an internet communication
13 device into a single hand-held product. (CAC ¶ 68.)
14

15 The price of each iDevice depends on the available memory on the device measured in
16 gigabytes ("GB"). (CAC ¶ 70.) The iDevices range from \$199 for a 16GB iPod Touch or
17 discounted iPhone to \$699 for the 64GB iPad. (CAC ¶¶ 70-73.) Every app takes up a portion of
18 the available memory on the iDevice depending on the size of the app. (*Id.*) Unlike many other
19 types of personal computers and telephones, the iDevices cannot be upgraded to add additional
20 memory. (CAC ¶ 147.) In addition, the rechargeable batteries on iDevices are not replaceable,
21 so once the battery will no longer hold a charge the iDevice becomes essentially inoperable.
22

23 (*Id.*)

24 The commercial success of the iPhone is based in large part on its function as an all-
25 purpose device one can carry in one's pocket. This, in turn, is directly tied to the availability of
26 thousands of software apps. In July 2008, Apple launched the "App Store" where customers can
27 shop for and acquire apps offered by Apple and third-party developers. (CAC ¶ 74.) When it
28 first launched, the App Store contained only about 500 apps. (CAC ¶ 75.) Today Apple boasts

1 700,000 apps in the App Store. (CAC ¶ 77.) Apple’s website tells consumers, “[t]he apps that
2 come with your iPhone are just the beginning. Browse the App Store to find hundreds of
3 thousands more. The more apps you download, the more you realize there’s almost no limit to
4 what your iPhone can do.” (CAC ¶ 75.) Apple makes similar claims regarding iPad and iPod
5 Touch. (CAC ¶ 76.)

6
7 Apple designed its iPhone, iPad and iPod Touch wireless mobile devices to accept apps
8 only from the App Store, making the App Store the exclusive source from which consumers may
9 obtain apps for their iDevices. (CAC ¶ 78, 173-177.) This exclusive source for apps is
10 consistent with Apple’s long notoriety for complete control over its products. (CAC ¶¶ 87, 173-
11 197.) Apple’s former CEO Steve Jobs publicly stated, “...our job is to take responsibility for the
12 complete user experience. And if it’s not up to par, it’s our fault, plain and simply.” (CAC ¶
13 87.)

14 As part of exerting this control over all apps, in order to offer an app for download in the
15 App Store, a third-party developer must be registered as an “Apple Developer” and agree to the
16 iOS Developer Agreement (the “IDA”) and the Program License Agreement (the “PLA”) with
17 Apple, as well as pay Apple a \$99 annual registration fee. (CAC ¶¶ 89, 181-197.) Apple then
18 controls the app development process. (CAC ¶¶ 91, 181-197.) For example, App developers
19 must buy and use Apple’s software development kit, which provides highly detailed guidelines
20 for app development. (CAC ¶ 91.) Apple provides app developers all of the pieces and
21 components pre-built they need to build iDevice apps; as a result, all apps were built, in part, by
22 Apple. (CAC ¶ 189.)

23 To get applications into the App Store, Apple requires developers to submit their app and
24 wait for approval or rejection by Apple (and rejected apps are given feedback on the reason they
25 were rejected so they can be modified and resubmitted). (CAC ¶ 90.) Apple has the sole
26 discretion over the app approval process and may reject a proposed app for any reason. (CAC ¶
27 90.) Apple may further unilaterally choose to cease distributing any app at any time and for any
28 reason. (CAC ¶ 193.) Apple has explicitly reserved the right to cease distributing any app that,
among other things, (i) breaches the terms and conditions of the licensing agreements, (ii)

1 provides Apple with inaccurate documents or information, or (iii) causes Apple (whether by
2 notification or otherwise) to believe that the app violates, misappropriates, or infringes the rights
3 of a third party. (CAC ¶ 90.) Apple even requires, by contract, that it serve as each app
4 developer's agent for its apps. (CAC ¶ 177.)

5 Apple therefore acts as a gatekeeper to the App Store and completely controls what is
6 available for users of iDevices. (CAC ¶¶ 91-96.) Indeed, when Apple first launched the App
7 Store, Steve Jobs stated, "[t]here are going to be some apps that we're not going to distribute.
8 Porn, malicious apps, apps that invade your privacy." (CAC ¶ 92.) Apple has also famously
9 refused to integrate Adobe Flash technology (which is utilized by many websites and without
10 which Apple Devices cannot access such content) despite users' requests, with Jobs explaining
11 (on Apple's website in April 2010) that Apple will not integrate Adobe's flash technology
12 because of reliability, security, and performance concerns.² (CAC ¶ 97.) Likewise, on April 20,
13 2011, the Company's current CEO, Timothy Cook, noted that users appreciate Apple's
14 gatekeeper function, stating "I think the user appreciates that Apple can take full responsibility
15 for their experience." (CAC ¶ 98.)

16 Apple has gone to great lengths to advertise and create the impression that its products
17 protect user privacy despite the development of apps by third parties. (CAC ¶¶ 64, 92, 94.)
18 Apple's policies prohibit apps from "transmit[ting] data about a user without obtaining the user's
19 prior permission and providing the user with access to information about how and where the data
20 will be used." (CAC ¶ 191.) According to Apple's extensive advertising campaign, its operating
21 system, iOS, "is highly secure from the moment you turn on your iPhone." (CAC ¶¶ 102-3.)
22 Apple makes similar claims with respect to the iPad and the iPod Touch. (CAC ¶ 103.)

23 Plaintiffs are 16 individuals who purchased iDevices from Apple prior to February 2012.
24 (CAC ¶¶ 16-32.) Before purchasing their iDevices, each Plaintiff was aware of Apple's
25 extensive advertising and public representations that the iDevices were secure. (CAC ¶ 32.)

26
27 ² The inability of iDevices to use Adobe Flash despite enormous public demand and
28 criticism is a testament to Apple's iron grip on the app market for its devices.

1 Two of the plaintiffs watched live blogs and web announcements led by Apple's co-founder and
2 then CEO Steven Jobs. (CAC ¶¶ 24, 31). These included representations such as that the App
3 Store does not permit apps that "violate Apple's developer guidelines including apps that violate
4 user privacy," that "Apple takes precautions . . . to safeguard your personal information against
5 loss, theft, and misuse, as well as against unauthorized access," that iDevices are "safe and
6 secure," and that "applications on the Device are 'sandboxed' so they cannot access data stored
7 by other applications." (CAC ¶¶ 121-123, 208-209.) Apple made these representations and
8 many others like them to encourage Plaintiffs and other members of the public to purchase
9 iDevices and to accept add-on apps from the App Store. (CAC ¶ 208.)

10 Plaintiffs relied upon Apple's representations and Apple's reputation for safety,
11 cultivated through Apple's extensive marketing and advertising campaigns. (CAC ¶¶ 32, 87-98,
12 99, 211.) The iDevices come with a built in "Contacts" app which permits the user to store
13 personal and private information about the user, his/her family, friends, business contacts or
14 anyone else. (CAC ¶ 159.) Akin to a rolodex or traditional "little black book," the Contacts of
15 each user reveals connections, associations and relationships that are unique to the owner of the
16 iDevice. (CAC ¶ 160.) Much like a company's customer lists, the investment of time, effort,
17 skill and creative energy used to build the user's unique address book has independent value,
18 including the time spent learning and building the contact address book, and the time spent
19 creating and inputting data and information and updating it. (CAC ¶¶ 160,165.) Private
20 Contacts address books are a highly valued surveillance target because companies can use such
21 address books to profit from and exploit emerging social media through advertising and/or
22 expanding their own user data bases. (CAC ¶¶ 168-171.) Similar to customer lists, telephone
23 numbers and email addresses of users are commodities that are available for sale in the
24 marketplace. (CAC ¶ 151.)

25 As a result of the sustained advertising assurances from Apple, each Plaintiff purchased
26 their iDevices with the expectation that they would be able to utilize the "Contacts" function and
27 download and utilize apps available through the App Store without compromising the safety or
28 exclusive control of the personal and private information. (CAC ¶ 32.) Had any Plaintiff known

1 that iDevices lacked these promised features, or that Apple designed the iDevices with known
2 vulnerabilities to unauthorized operations from Apple-issued (third-party) apps, Plaintiffs would
3 not have accepted add-on apps from Apple or the App Store, and would have paid less for his or
4 her iDevice or not purchased it. (CAC ¶¶ 32, 64, 125-127.)

5 During the timeframe at issue, Plaintiffs downloaded a number of apps from the App
6 Store, including apps manufactured by the Defendant App Developers here. (CAC ¶¶ 16, 19,
7 28.) These include some of the most popular “free” apps, such as Facebook, Twitter, Instagram,
8 and Yelp!, as well as popular games like Angry Birds and Cut the Rope which had both free and
9 paid versions. (Id.) Plaintiffs also maintained substantial private data in the Contacts app on
10 their iDevice; each Plaintiff had more than one hundred contacts in their iDevice Contacts at all
11 relevant times. (CAC ¶ 151.)

12 Unbeknownst to Plaintiffs, many popular apps, including the ones at issue here, are not
13 benign social media tools or games. They are active surveillance devices designed to intercept
14 users’ private address book information (including names and contact information), location
15 dates, photographs, and videos without the users’ knowledge or consent. (CAC ¶¶ 62, 107-119.)
16 This surveillance took two forms.

17 First, some apps simply took the data without even a pretense of permission. For
18 example, in early February 2012, it was revealed that defendant Path’s eponymous app was
19 uploading data stored on users’ iDevices (including address book and calendar) to its servers,
20 causing Path’s CEO to issue an apology to Path users. (CAC ¶ 110.)

21 Second, other apps misled users into “consenting” to the theft of their data through
22 features that offered to “find friends” or otherwise identify people the users might know who
23 used the same app. (CAC ¶¶ 62, 108, 236, 317.) The App Developers lean heavily on this
24 “friend finder” consent in their motion, never revealing to the Court that the so-called permission
25 was not a request to copy the Contacts or to send a copy of those contacts to the App
26 Developers’ computers. (Id.) Users who were asked whether they wanted to know if their
27 friends, for example, also played Angry Birds or used Twitter were never told that agreeing to
28

1 receive that “service” would result in the App Developer obtaining a copy of all of their private
2 Contacts. (CAC ¶ 108.)

3 The apps then transmitted the stolen app copies from the iDevices to the App Defendants’
4 own computers. (CAC ¶¶ 262, 307, 322, 549.) That transmission not only stole the address
5 books, it also used system resources, including battery life, WiFi bandwidth, or cellular
6 telephone time. (CAC ¶ 147.) Battery life is particularly an issue with iDevices because the
7 battery on an iDevice cannot be replaced. (CAC ¶ 338.) Because any use of a battery drains it,
8 and rechargeable batteries have a finite number of charges they will take, any use of an iDevice
9 necessarily decreases not only the life of the battery but of the device itself. (*Id.*) Moreover,
10 many of these surreptitious transmissions appear to have been made without industry standard
11 encryption. (CAC ¶ 341.) Sending this private data on an unencrypted radio broadcast (by either
12 WiFi or cellular network) subjects the user to a significant risk of interception by one of many
13 other actors in the surveillance economy.⁴ (*Id.*) Because no user was warned that the
14 transmission would occur, there is no way for any user to determine how much of his or her
15 private data was acquired by third parties as a result of these unauthorized transmissions. (CAC
16 ¶¶ 264, 361.) Thus each plaintiff, and other users of the same apps, was damaged in a number of
17 ways by the App Developers’ surreptitious copying of their address books. (CAC ¶¶ 129-152.)

18 All of this conduct was contrary to Apple’s representations; indeed, Apple had repeatedly
19 assured the consuming public that this type of interception of private data was impossible on an
20 iDevice and that Apple scrupulously monitored all apps before placing them on the app store.
21 Contrary to their marketing promises and unbeknownst to Plaintiffs, Apple sold Plaintiffs
22 defective iDevices lacking these promised security features. (CAC ¶ 128.) It then facilitated the
23 distribution of the spyware apps which took control of Plaintiffs’ iDevices and secretly relayed
24 Plaintiffs’ valuable private Contacts to the App Defendants via the Internet and in an unsecured
25

26 ⁴ For example, Google is in significant legal trouble after it was revealed that Google’s
27 mapping vehicles were gathering information from the WiFi of unsuspecting homes as they
28 drove by. (CAC ¶ 119.) See Joffe v. Google, Inc., 729 F.3d 1262, 1264 (9th Cir. 2013).

1 manner. (Id.) Apple is thus jointly responsible for the harm caused to each Plaintiff, as well as
 2 for over-charging Plaintiffs for a device that did not perform as represented. (CAC ¶ 689.)

3 **III. ARGUMENT**

4 **A. SECTION 230 OF THE CDA DOES NOT BAR PLAINTIFFS' CLAIMS AGAINST** 5 **APPLE**

6 **1. The Motion to Dismiss Stage is Not a Proper Time to Resolve** 7 **Whether the CDA Applies**

8 Apple's reliance on Section 230(c) of the CDA⁵ to dismiss this action is premature and
 9 has already been addressed by Judge Rogers in the Pirozzi I Action. See Pirozzi v. Apple Inc.,
 10 913 F. Supp. 2d 840, 849 (N.D. Cal. 2012). In Pirozzi I, Judge Rogers rejected the very same
 11 argument that Apple now makes before this Court – that Plaintiffs' claims against Apple for the
 12 content of third party apps are barred by the CDA – and found that:

13 *Plaintiff's claims are not predicated solely upon Apple's*
 14 *approving and distributing Apps via its online App Store;*
 15 *Plaintiff also seeks to hold Apple liable for representations made*
 16 *by Apple itself. As Apple acknowledges, Plaintiff's claims include*
 17 *"allegations that Apple somehow misled Plaintiff as to the 'nature*
 18 *and integrity of Apple's products.'" (Mot. 18.) To the extent that*
 19 *Plaintiff's claims allege that Apple's misrepresentations induced*
 20 *Plaintiff to purchase an Apple Device, those claims do not seek to*
 21 *hold Apple liable for making Apps available on its website. In*
 22 *that context, even if Apple acts as an "interactive computer*
 23 *service," Plaintiff seeks to hold it liable as the "information*
 24 *content provider" for the statements at issue.*

25 Id. at 849 (emphasis added).

26 As Judge Rogers observed, Apple's reliance on Carafano v. Metrospalsh.com, Inc., 339
 27 F.3d 1119, 1123 (9th Cir. 2003),⁶ was misplaced because "[u]nlike the findings in Carafano,

28 ⁵ Although Apple couches the CDA as providing "unconditional immunity," the Ninth
 Circuit has held that "neither this subsection [Section 230 (c)] nor any other declares a general
 immunity from liability deriving from third-party content. . . . 'Subsection (c)(1) does not
 mention 'immunity' or any other synonym.' . . . [I]t appears that subsection (c)(1) only protects
 from liability (1) a provider or user of an interactive computer service (2) whom a plaintiff seeks
 to treat . . . as a publisher or speaker (3) of information provided by another information content
 provider." Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1100-1 (9th Cir. 2009).

⁶ Indeed Carafano, a defamation and right of publicity case involving a dating website, was
 decided on a motion for summary judgment, not on a motion to dismiss. Carafano, 339 F.3d
 1121. Central to the Ninth Circuit's decision was that – unlike Apple here – the dating website
 Case No. : 13-cv-00453-JST -9- OPP'N TO APPLE MOT. TO DISMISS

1 supra, as to the role of Matchmaker.com for the content of information, if Apple is responsible
 2 for the ‘creation or development of [the] information’ at issue, then Apple functions as an
 3 ‘information content provider’ unprotected by the CDA.” Id. at 849.

4 Further, Judge Rogers held that application of the CDA is an affirmative defense and
 5 therefore concluded that “it is premature to decide whether CDA bars Plaintiff’s claims.” Id.
 6 Judge Rogers’ holding in Pirozzi I is in line with holdings of courts in this circuit and elsewhere:
 7 The CDA is an affirmative defense that turns on interpretation of facts, and as such should not be
 8 resolved through a 12(b)(6) motion. See, e.g., Swift v. Zynga Game Network, Inc., 09-05443
 9 SBA, 2010 WL 4569889, *6 (N.D. Cal. Nov. 3, 2010) (“Given the limited nature of a Rule
 10 12(b)(6) challenge, the Court cannot determine, at this stage, whether Adknowledge is entitled to
 11 CDA immunity. It would be improper to resolve this issue on the pleadings and the limited
 12 record presented.”) (citing Perfect 10, Inc. v. Google, Inc., 04-9484, 2008 WL 4217837, *8 (C.D.
 13 Cal. July 16, 2008) (“preemption under the CDA is an affirmative defense that is not proper to
 14 raise in a Rule 12(b)(6) motion”)).

15 The courts that have considered the CDA at the motion to dismiss stage have only done
 16 so “where the defense is ‘apparent from the face of the [c]omplaint.’” Holomaxx Tech.s v.
 17 Microsoft Corp., 783 F. Supp. 2d 1097, 1103 (N.D. Cal. 2011). Unlike Holomaxx, Plaintiffs
 18 here do not concede that Apple is an “interactive computer service” nor is the application of the
 19 CDA apparent from the face of the complaint.⁷ Thus, Apple’s CDA arguments should not be
 20 considered at this time.

21
 22 Matchmaker.com “was not responsible, even in part” for the content created by users of the
 23 website. Id. at 1124. As provided further below the facts in this action are entirely different
 24 from of those in Carafano. As alleged in the CAC, Apple was responsible for the content of the
 25 third party apps (CAC ¶¶ 87-91, 181-94; 212-14) – a fact that a later panel of the Ninth Circuit
 26 found to be sufficient to prevent CDA immunity. See Fair Hous. Council of San Fernando
 27 Valley v. Roommates.com, LLC, 521 F.3d 1157, 1167-68 (9th Cir. 2008). The Roommates.com
 28 Court also noted that the Ninth Circuit “disavow[s] any suggestion that Carafano holds an
 information content provider *automatically* immune so long as the content originated with
 another information content provider.” Id. at 1171.

⁷ Apple’s reliance on Evans v. Hewlett-Packard Co., 13-02477 WHA, 2013 WL 5594717,
 *3 (N.D. Cal. Oct. 10, 2013), is misplaced because, unlike Judge Rogers, the Evans court found
 that it did not need a factual record to determine whether CDA immunity was appropriate on the
 Case No. : 13-cv-00453-JST -10- OPP’N TO APPLE MOT. TO DISMISS

1 Moreover, without discovery, it is premature to conclude that the App Store is an
 2 “interactive computer service” that is even under the purview of the CDA. For example, the App
 3 Store is accessed through a preprogrammed app that comes standard on each iDevice (CAC ¶¶
 4 61, 173), and is therefore not a traditional website like those at issue in Roommates.com and
 5 Carafano.⁸ In addition, Apple improperly reaches outside the four corners of the CAC to allege
 6 (without any factual support) that its app development tools – the SDK – also fall within the
 7 CDA because the SDK is available to app developers online. Whether SDK is available online
 8 and how developers use the SDK to develop apps is a factual matter that is not before the Court
 9 on the motions to dismiss. Furthermore, these facts do not alter Apple’s involvement in
 10 developing the third-party apps through creation and distribution of the SDK kit and Apple’s app
 11 review process. See, e.g., Roommates.com, 521 F.3d at 1165 (finding that an online website
 12 service was also an information content provider not shielded by the CDA and noting that “the
 13 fact that users are information content providers does not preclude Roommate from *also* being an
 14 information content provider by helping ‘develop’ at least ‘in part’ the information in the
 15 profiles.”).

16
 17 **2. Section 230(c)(1) Provides No Defense to Apple Because Plaintiffs’**
 18 **Claims Arise From Apple’s Conduct, Not From Passive Transmission**
 19 **of Third Party Content**

20 Congress enacted the CDA in response to a New York state court decision⁹ that found an
 21 internet service provider strictly liable for allowing a third party to post a libelous message on

22 facts presented. Indeed, in denying plaintiff’s request to amend his trademark infringement
 23 claims, the Evans Court distinguished Pirozzi I, noting that Judge Rogers found that Pirozzi
 24 claimed that Apple “somehow misled Plaintiff as to the nature and integrity of [the defendant’s]
 product” while in Evans there was no debate regarding how the product was described. Id.

25 ⁸ For this reason, Atl. Recording Corp. v. Project Playlist, Inc., 603 F. Supp. 2d 690
 26 (S.D.N.Y. 2009) is distinguishable. In that case, a website provided links to other, third-party
 27 websites from which users could download songs. Id. at 693-94. In contrast, here, users access
 the App Store – an integrated app – through their iDevice.

28 ⁹ Stratton Oakmont, Inc. v. Prodigy Services Co., 31063/94, 1995 WL 323710 (N.Y. Sup.
 Ct. May 24, 1995).

1 one of its message boards. Section 230(c)(1) provides: “No provider or user of an interactive
2 computer service shall be treated as the publisher or speaker of any information provided by
3 another information content provider.” 47 U.S.C. § 230(c)(1). The CDA was enacted “to
4 promote the free exchange of information and ideas over the Internet and to encourage voluntary
5 monitoring for offensive or obscene material.” Carafano, 339 F.3d at 1122. The statute was
6 never intended to provide blanket immunity for all acts by interactive computer service
7 providers. See Roommates.com, 521 F.3d at 1164 (“The [CDA] was not meant to create a law-
8 less no-man’s-land on the Internet.”).

9 Apple attempts to repurpose the CDA from the promotion of free speech to the
10 immunization of theft. Plaintiffs’ claims are not based on “content” but rather on *conduct*. Nor
11 are Plaintiffs attempting to hold Apple strictly liable for merely “publishing” false
12 advertisements from other persons. Rather, Plaintiffs are seeking to impose liability for Apple’s
13 active orchestration of and participation in a scheme that allows apps to steal users’ private
14 information.

15 By its terms, the grant of immunity found in Section 230(c)(1) applies *only* if the
16 interactive computer service is not also an “information content provider.” See also Zynga, 2010
17 WL 4569889 at *3 (“This grant of immunity does not apply if the interactive computer service
18 provider is also an ‘information content provider’ which is defined as someone who is
19 ‘responsible, *in whole or in part*, for the creation or development of’ the offending content.”
20 (emphasis in original)); Roommates.com, 521 F.3d at 1162 (holding that CDA immunity
21 “applies only if the interactive computer service provider is not also an ‘information content
22 provider’”); Batzel v. Smith, 333 F.3d 1018, 1033 (9th Cir. 2003); Fraley v. Facebook, Inc., 830
23 F. Supp. 2d 785, 801-802 (N.D. Cal. 2011) (CDA immunity didn’t apply because “[a]lthough
24 Facebook meets the definition of an interactive computer service under the CDA . . . , in the
25 context of Plaintiffs’ claims, it also meets the statutory definition of an information content
26 provider.”).

27 Apple incorrectly asserts that the CAC details nothing more than Apple’s provision of
28 neutral tools to app developers. (Apple MTD at 14.) However, as alleged in the CAC, Apple

1 was not merely a passive participant in the development and distribution of apps on the iDevices.
 2 Rather, as alleged in the CAC, Apple was a very active, and indeed controlling participant. (CAC
 3 ¶¶ 89-91, 181-94.) As such, Apple cannot seek refuge under the CDA from the consequences of
 4 its conduct.

5 As the Ninth Circuit has held, “the party responsible for putting information online may
 6 be subject to liability, even if the information originated with a user.” Roommates.com, 521
 7 F.3d at 1165; id. at 1171 (“even if the data are supplied by third parties, a website operator may
 8 still contribute to the content’s illegality and thus be liable as a developer. Providing immunity
 9 every time a website uses data initially obtained by third parties would eviscerate the exception
 10 to section 230 for ‘develop[ing]’ unlawful content ‘in whole or in part’). Moreover, the Zynga
 11 Court observed:

12 In passing Section 230, Congress sought to allow interactive
 13 computer services ‘to perform some editing on user-generated
 14 content without thereby becoming liable for all defamatory or
 15 otherwise unlawful messages that they didn’t edit or delete.’ ‘In
 16 other words, Congress sought to immunize the removal of user-
 17 generated content, not the creation of content’ As noted by the
 18 Ninth Circuit, ‘[i]ndeed, the section is titled ‘Protection for ‘good
 19 samaritan’ blocking and screening of offensive material’ ... the
 20 substance of section 203(c) can and should be interpreted
 21 consistent with its caption.’

22 2010 WL 4569889 at *4 (citing Roommates.com, 521 F.3d at 1163).

23 Zynga is particularly instructive here. In that case, plaintiff, a “virtual world”
 24 game created by the defendant game-developer Zynga, brought a suit for violation of the UCL
 25 and CLRA, based on allegedly fraudulent in-game special offers from third-parties. Id. at *1-3.
 26 Plaintiff alleged that Zynga generated its revenue through sale of virtual currency to players. Id.
 27 at *1. Among the ways players could earn virtual currency, was through third-party special
 28 offers. Id. Plaintiff alleged that these special offers (which were integrated into the game by
 Zynga and an aggregator¹⁰) were misleading and resulted in users subscribing to unwanted goods
 or services. Id.

¹⁰ According to Zynga, the game-developer partnered with an aggregator, or an
 intermediary, to create the interfaces through which users could receive the third-party special
 offers. Id. at *1, *6.

1 Although Zynga argued that it was entitled to immunity under the CDA and sought to
 2 dismiss plaintiff's complaint, the Court denied its motion as premature because the complaint
 3 "alleges facts which, if proven, could support the conclusion that [Zynga] was responsible, in
 4 whole or in part, for creating or developing the special offers at issue." Id. at *5.

5 The same holds true here. Plaintiffs sufficiently allege that Apple participated at least in
 6 part in the development of the third-party apps distributed to class members on the iDevices that
 7 led to their private information being uploaded without consent. (CAC ¶¶ 89-91; 181-94; 212-
 8 14.)¹¹ And there is no question that Apple had a hand in making the apps usable or available to
 9 purchasers of the iDevices. As such, Apple is not immune from liability.

10 Plaintiffs have alleged sufficient facts under Roommates.com and Zynga to demonstrate
 11 that Apple may be "responsible, in whole or in part, for the creation or development of" the apps.
 12 Like Zynga, Apple has created a product (the iDevices) whose functionality and popularity is
 13 dependent on users' downloading third-party apps from the App Store. In Apple's own words,
 14 "[t]he apps that come with your iPhone are just the beginning. Browse the App Store to find
 15 hundreds and thousands more. The more apps you download, the more you realize there's
 16 almost no limit what your iPhone can do." (CAC ¶¶ 75-76.) Moreover, the CAC alleges that the
 17 "apps are an integral part of the iDevices and have propelled Apple and iDevices' popularity."
 18 (CAC ¶ 83.) Thus, Apple encourages purchasers and users of iDevices to download third-party
 19 apps because, as alleged in the CAC, these apps help bolster the company's popularity and
 20 therefore generate Apple's revenue, not just through sale of apps in the App Store, but through
 21 sales of the iDevices themselves. (CAC ¶¶ 59, 70-73, 79-86, 176, 450, 473.)

22 Apple further controls the entire app design process and has ultimate control over what
 23 apps are sold at the App store. (CAC ¶¶ 89-91; 181-94; 212-14.) Indeed, as provided above,
 24

25
 26 ¹¹ Numerous courts have denied defendants immunity under the CDA based on conduct.
 27 See Fraley, 830 F. Supp. 2d at 802 (finding that even though third parties "are information
 28 content providers does not preclude [Facebook] from *also* being an information content provider
 by helping 'develop' at least 'in part' the information'" and that Facebook's actions went
 "beyond editing user-created content—such as by correcting spelling, removing obscenity or
 trimming for length." (internal citations omitted)).

1 these apps, whether manufactured by Apple or by third-parties, are a key aspect of the device
 2 itself. Apple further designed the iDevices “to accept apps only from Apple’s App Store,
 3 making Apple’s App Store the exclusive source from which consumers may obtain apps for their
 4 iDevices.” (CAC ¶¶ 60, 78, 88, 91, 174, 182.) Apple even voids the warranty on any iDevice if
 5 its user modifies the operating system’s restriction on download only from the App Store. (CAC
 6 ¶ 88.)

7 Nor is Apple immune under the CDA for failure to warn consumers. (Apple MTD at 15.)
 8 Apple’s misstatements and omissions concerning the iDevices do not pertain just to conduct of
 9 third parties; Plaintiffs seek to hold Apple liable for statements that Apple made about the
 10 *functionality* of the iDevices themselves as well as Apple’s review process (CAC ¶¶ 102, 455-57,
 11 471, 511, 520). Thus, with respect to Apple’s statements regarding its own product, “even if
 12 Apple acts as an ‘interactive computer service,’ Plaintiff[s] seek[] to hold it liable as the
 13 ‘information content provider’ for the statements at issue.” Pirozzi I, 913 F. Supp. 2d at 849.
 14 Apple’s cited authority is therefore inapposite because these cases involve failure to warn about
 15 third party conduct or products, not misstatements and omissions concerning the defendant’s
 16 own product.

17 18 **3. Section 230(c)(2) Provides No Defense to Apple Because Apple is not Being Sued for Blocking Content**

19 Finally, Apple is not entitled to a separate affirmative defense under § 230(c)(2) because
 20 that section deals with liability for *blocking* certain content, not failure to block. See 47 U.S.C. §
 21 230(c)(2) (providers of an interactive computer service will not be held liable for “any action
 22 voluntarily taken in good faith to restrict access to or availability of material that the provider or
 23 user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise
 24 objectionable, whether or not such material is constitutionally protected” or “any action taken to
 25 enable or make available to information content providers or others the technical means to
 26 restrict access to material described in paragraph (1)”).

27 For example, in Batzel v. Smith, a panel of the Ninth Circuit noted in a footnote:

28 § 230(c)(2) further encourages good samaritans by protecting
 service providers and users from liability for claims arising out of

1 the removal of potentially “objectionable” material from their
 2 services. See § 230(c)(2). This provision insulates service
 3 providers from claims **premised on the taking down of a**
 4 **customer’s posting** such as breach of contract or unfair business
 practices. Cf. 17 U.S.C. § 512(g)(1)(providing similar protection
 for service providers who take down material alleged to violate
 copyright laws);H.R.Rep. No. 105-551, at 25 (1998).

5 Batzel, 333 F.3d at 1030 n.14 (emphasis added); see also Zango, Inc. v. Kaspersky Lab, Inc., 568
 6 F.3d 1169, 1117 (9th Cir. 2009) (“what § 230(c)(2)(B) *does* mean to do is to immunize any
 7 action taken to enable or make available to others the technical means to restrict access to
 8 objectionable material”)(emphasis in original); id. at 1116 (“§ 230(c)(2)(B) provides protection
 9 for ‘any action taken to enable or make available. . .the technical means to restrict access’ to
 10 material covered by § 230(c)(2)(A)”); Holomaxx Tech., 783 F. Supp. 2d 1097 (plaintiff sued
 11 defendant Internet service provider for blocking its emails).

12 Apple’s only case to the contrary is an out-of-circuit opinion that does not substantively
 13 analyze subsection (c)(2) because it found that section (c)(1) was met. See Doe v. MySpace,
 14 Inc., 474 F. Supp. 2d. 843, 850 (W.D. Tex. 2007), aff’d 528 F.3d 413, 421 (5th Cir. 2008).¹²
 15 Apple’s reliance on the Ninth Circuit’s decision in Barnes is also misplaced. The Barnes court
 16 did not consider whether Yahoo! had an affirmative defense under 230(c)(2) and instead held
 17 that Yahoo!’s failed attempt to block objectionable content fell under the publisher function of
 18 Section 230(c)(1) and barred liability on that basis alone. Id. at 1105, 1109. This provides no
 19 support for Apple’s claim here.

20
 21 **B. THIS COURT CLEARLY HAS JURISDICTION OVER THIS ACTION BECAUSE**
PLAINTIFFS HAVE STANDING TO PURSUE THEIR CLAIMS AGAINST APPLE

22 To have standing under Article III, a plaintiff need only show that (1) it has suffered an
 23 injury in fact; (2) the injury is fairly traceable to the defendants’ actions; and (3) the injury will
 24 likely be redressed by a favorable decision. Lujan v. Defenders of Wildlife, 504 U.S. 555, 560-
 25

26
 27 ¹² Indeed a panel of the Fifth Circuit that affirmed the Western District of Texas Court’s
 28 decision did so on the basis of 230(c)(1) and never reached the issue of whether the lower Court
 properly applied 230(c)(2). See Doe v. MySpace, Inc., 528 F.3d 413, 422 (5th Cir. 2008).

1 61 (1992). The “injury” requirement does not, however, mean that Plaintiffs have to win their
 2 claim at the beginning of the lawsuit:

3 “Injury in fact” [simply] reflects the statutory requirement that a
 4 person be “adversely affected” or “aggrieved,” and it serves to
 5 distinguish a person with a direct stake in the outcome of a
 litigation—even though small—from a person with a mere interest
 in the problem.

6 United States v. Students Challenging Regulatory Agency Procedures, 412 U.S. 669, 690 n. 14
 7 (1973). “The purpose of standing doctrine is to ensure that ‘plaintiff’s claims arise in a ‘concrete
 8 factual context’ appropriate to judicial resolution and that ‘the suit has been brought by a proper
 9 party.’ The ‘injury-in-fact’ analysis is not intended to be duplicative of the analysis of the
 10 substantive merits of the claim. Haskins v. Symantec Corp., 13-CV-01834-JST, 2013 WL
 11 4516179, *3 (N.D. Cal. Aug. 23, 2013) (quoting Arakaki v. Lingle, 477 F.3d 1048, 1059 (9th
 12 Cir. 2007) (internal reference omitted)).

13 Apple argues at pp. 17-23 of its brief that Plaintiffs lack Article III standing to bring their
 14 claims. Apple, however, runs roughshod over the standards governing a standing motion.
 15 Standing “in no way depends on the merits of the plaintiff’s contention that particular conduct is
 16 illegal,” Warth v. Seldin, 422 U.S. 490, 500 (1975), and “does not require analysis of the
 17 merits.” Equity Lifestyle Props., Inc. v. County of San Luis Obispo, 548 F.3d 1184, 1189 n.10
 18 (9th Cir. 2008). For Article III standing, “[a]t the pleading stage, general factual allegations of
 19 injury resulting from the defendant’s conduct may suffice, for on a motion to dismiss we
 20 presum[e] that general allegations embrace those specific facts that are necessary to support the
 21 claim.” Lujan, 504 U.S. at 561 (internal citations omitted).¹³

22
 23
 24
 25 ¹³ See also Fraley, 830 F. Supp. 2d at 800 (“Defendant would have the Court evaluate the
 26 merits of Plaintiffs’ § 3344 claim before even allowing Plaintiffs through the courthouse door.
 27 But as the Ninth Circuit recently reminded, ‘standing analysis, which prevents a claim from
 28 being adjudicated for lack of jurisdiction, [may not] be used to disguise merits analysis, which
 determines whether a claim is one for which relief can be granted if factually true.’”) (quoting
Catholic League for Religious and Civil Rights v. City & Cnty. of S.F., 624 F.3d 1043, 1049 (9th
 Cir. 2010) (en banc)).

2. Plaintiffs' Injunctive and Statutory Claims Create Standing

Apple does not claim that Plaintiffs lack a personal stake in this dispute.¹⁶ Instead, Apple makes “standing” arguments based on its assertion that it did not harm the Plaintiffs. That is a disguised merits attack, not a standing issue. Before responding to Apple’s specific arguments, Plaintiffs will first identify the claims and remedies Apple ignores in its motion.

First, Apple ignores Plaintiffs’ requests for prospective injunctive relief to stop the challenged misconduct. “To have standing to assert a claim for prospective injunctive relief, a plaintiff must demonstrate ‘that he is realistically threatened by a repetition of [the violation].’” Melendres v. Arpaio, 695 F.3d 990, 997 (9th Cir. 2012). Because Apple’s challenged activity was deliberate and ongoing, it will necessarily continue unless enjoined. Nicacio v. U.S. I.N.S., 797 F.2d 700, 702 (9th Cir. 1985) (noting that on claims for prospective injunctive or equitable relief, “[t]he possibility of recurring injury ceases to be speculative when actual repeated incidents are documented” and establishes standing to redress that prospective harm) (overruled on separate grounds in Hodgers-Durgin v. de la Vina, 199 F.3d 1037, 1045 (9th Cir. 1999)).

Second, Apple ignores Plaintiffs’ claims for statutory damages. (CAC ¶ 609.) “[T]he injury required by Article III can exist *solely* by virtue of ‘statutes creating legal rights, the invasion of which creates standing.’” Edwards v. First American Corp., 610 F.3d 514, 517 (9th Cir. 2010) (quoting Warth, 422 U.S. at 500), writ dism’d, 132 S. Ct. 2536 (June 28, 2012) (per curiam). Thus, if any statute prohibits Apple’s conduct and allows for a civil recovery, Plaintiffs have demonstrated an injury sufficient to satisfy Article III. Id. Here, Plaintiffs allege the violation of numerous statutes as discussed throughout the CAC.

¹⁶ In a putative class action like this one, standing need only be established for one class representative. As this Court recently reaffirmed, “[t]he Ninth Circuit’s ‘[standing] law keys on the representative party, not all of the class members, and has done so for many years.’” Lilly v. Jamba Juice Co., 13-CV-02998-JST, 2013 WL 6070503, *2 (N.D. Cal. Nov. 18, 2013) (citing Stearns v. Ticketmaster Corp., 655 F.3d 1013, 1021 (9th Cir. 2011) cert. denied, 132 S.Ct. 1970 (U.S. 2012); see also Bates v. United Parcel Serv., Inc., 511 F.3d 974, 985 (9th Cir. 2007) (en banc) (‘[i]n a class action, standing is satisfied if at least one named plaintiff meets the requirements’)).

3. Plaintiffs Have Standing to Bring the Non-Statutory Claims

In Pirozzi v. Apple, Inc., 12-CV-01529, 2013 WL 4029067, *3-*5 (N.D. Cal. Aug. 5, 2013) (“Pirozzi II”), this court held that the allegations by Plaintiff Pirozzi (one of the plaintiffs in this CAC) that she overpaid for the iDevice in reliance upon Apple’s misrepresentations were sufficient to establish Article III standing. Adopting Judge Rogers’ opinion in Pirozzi I, this court affirmed that Pirozzi’s allegation of overpayment based on misrepresentations “is enough to satisfy Article III’s injury-in-fact requirement.” Id. at *4. Here, the CAC incorporates Pirozzi’s allegations as to all Plaintiffs. (CAC ¶¶ 28, 32, 102.) Applying Pirozzi II, these allegations are sufficient to meet Article III standing requirements. Accord Goodman v. HTC America, Inc., 11-1793 MJP, 2012 WL 2412070, *6 (W.D. Wash. Jun. 26, 2012) (plaintiffs’ assertion that they overpaid for their smartphones due to the manufacturer’s misleading statements met Article III standing requirement); Donohue v. Apple, Inc., 11-cv-05337 RMW, 2012 WL 1657119, *3-*5 (N.D. Cal. May 10, 2012) (citing Kwikset v. Superior Court, 51 Cal.4th 310, 323 (2011)) (plaintiff met Article III standing requirement when he alleged that his smartphone’s signal gauge was not as accurate as initially represented by the manufacturer and that knowledge of this issue would have impacted his decision to purchase the phone); Womack v. Nissan N. Am., Inc., 550 F. Supp. 2d 630, 635 (E.D. Tex. 2007) (decreased value of automobile with inflated mileage conferred standing); see also Lujan, 504 U.S. at 560 n.1 (“by particularized, we mean that the injury must affect the plaintiff in a personal and individual way”).

Apple ignores Pirozzi II, and makes a series of baseless arguments against standing. First, Apple argues that Plaintiffs have not “plausibly” alleged that any of their address book information was actually uploaded by the App Defendants without their consent. (Apple MTD at 18:11-12.) That is nonsense. Plaintiffs repeatedly make that allegation. It is what this whole case is about. (CAC ¶¶ 7, 24, 31, 62, 108, 110, 112, 123, 138, 240, 261, 302, 320, 359, 371, 394, 401.)

1 Apple further urges that any such conduct by the App Defendants is “not traceable to the
2 conduct of Apple.” (Apple MTD at 18:13-20.) This also ignores the detailed allegations
3 concerning Apple’s control over app development and distribution. Apple created and
4 completely controls every aspect of the “Apple ecosystem”; designs the iDevices to permit
5 surreptitious uploads by app developers; completely controls and regulates the design,
6 development and approval of the apps; requires that all apps be distributed on the App Store,
7 which is owned by Apple and where Apple receives a majority of the revenue paid for apps; and
8 represents to the potential purchasers that it has approved the apps and that they meet Apple’s
9 standards on safety and security. (See, e.g., CAC, ¶¶ 87-106.) Apple is also the App
10 Defendants’ designated agent for marketing and deploying each app. (CAC ¶ 145.)

11 Apple’s reliance upon In re iPhone Application Litig., 11-MD-02250-LHK, 2011 WL
12 4403963 (N.D. Cal Sept. 20, 2011) (“In re iPhone I”), is misplaced. Judge Koh’s subsequent
13 opinion in In re iPhone Application Litig., 844 F. Supp. 2d 1040, 1055-56 (N.D. Cal. 2012) (“In
14 re iPhone II”) holds that Apple’s control over every aspect of the ecosystem, including that
15 “Apple has designed its products to allow consumers’ personal information to be transmitted to
16 third parties,” is sufficient to establish that the injury was traceable to Apple as well, citing
17 Hepting v. AT&T Corp., 439 F. Supp. 2d 974, 1001 (N.D. Cal. 2006) (allegations that AT&T
18 actively partnered to intercept and monitor customer phone lines was sufficient to establish
19 standing).

20 Apple next asserts that none of the plaintiffs has identified any representations made by
21 Apple that was material to his or her decision to purchase any iPhone. (Apple MTD at 18:21-
22 19:4.) This misstates the record. The Court has already found that Pirozzi’s “primary
23 misrepresentation theory satisfies Article III standing, as she adequately pled specific
24 misrepresentations upon which she relied, causing her economic injury.” Pirozzi II, 2013 WL
25 4029067 at *5. Not only does the CAC contain the same allegations as were found sufficient by
26 this court in Pirozzi II (e.g., each Plaintiff visited Apple’s website and viewed Apple’s online, in-
27 store, and/or television advertisements” and the Apple website contained specific assurance of
28

1 safety of the users' contact information) (CAC, ¶¶ 32, 102),¹⁷ but this court has specifically
 2 rejected these types of arguments in similar cases. For example, in Clancy v. The Bromley Tea
 3 Co., No. 12-cv-03003-JST, 2013 WL 4081632, *6 (N.D. Cal., Aug. 9, 2013), the court held that
 4 the plaintiff specifically pleaded that he read statements on the defendant's website prior to
 5 purchasing the tea products, which "should be sufficient under normal pleading standards to
 6 establish Article III standing." In Haskins, 2013 WL 4516179 at *3, the court observed that
 7 Defendant's argument that Plaintiff cannot show that she was deprived of the benefit of the
 8 bargain because she has not identified any representations on which she relied "is an argument
 9 that Plaintiff has failed to state a claim rather than an argument about Plaintiff's standing. It is
 10 sufficient that the facts, as pled, establish that she has suffered harm." Id. "[T]here is nothing
 11 about her relationship to the purported injury that renders the Court without jurisdiction to
 12 determine the question." Id.

13 Alternatively, Apple seeks to attack the factual veracity of Plaintiffs' pleadings,
 14 submitting two declarations in an attempt to show that three of the Plaintiffs (Hoffman, Pirozzi
 15 and Varner) (CAC, ¶¶ 24, 28, 31) did not rely upon on any alleged misrepresentation. Apple
 16 claims that its business records show that (Hoffman and Varner) purchased their iPhones and
 17 downloaded the apps months before a specific statement they remember seeing was published.
 18 (Apple MTD at 18.) Apple also suggests that Pirozzi's allegation that she viewed the
 19 misrepresentation on the website should be discredited, claiming it would require "extraordinary
 20 inferences," because she would have had to navigate a maze to get to the page containing the
 21 alleged misrepresentation on the website.

22 These arguments are readily dismissed. *All* fourteen Plaintiffs—not just three—allege
 23 that they viewed and relied upon Apple's misrepresentations before purchasing their iDevices,
 24

25 ¹⁷ Apple's reliance (MTD at p. 18) upon Cattie v. Walmart Stores, Inc., 504 F. Supp. 2d
 26 939, 946-49 (S.D. Cal. 2007) and Williamson v. Reinalt-Thomas Corp., 11-CV-03548-LHK,
 27 2012 WL 1438812, *15 (N.D. Cal. Apr. 25, 2012) is misplaced. In Cattie, the court noted there
 28 was no evidence that the plaintiff ever opened the product or was dissatisfied with it. In
Williamson, the court concluded that an incidental \$2.50 tire disposal fee was not an important
 term upon which plaintiff relied. Here, by contrast, Plaintiffs allege that the security of their
 mobile address book was extremely private and important.

1 including those not only on the website, but in-store and television advertisements as well (CAC,
 2 ¶ 32).¹⁸ Disputes as to which of a series of substantially similar statements each plaintiff saw are
 3 not grounds to grant a motion to dismiss.

4 Finally, Apple argues that Plaintiffs are “required to allege ‘something more’ than
 5 ‘overpaying for a ‘defective’ product’” where the wrong stems from allegations about
 6 insufficient performance or how a product functions. (Apple MTD at 20:3-28.) This argument
 7 again ignores the allegations in the Complaint and applicable law.¹⁹

8 A similar claim was rejected in Kosta v. Del Monte Corp., 12-CV-01722, 2013 WL
 9 2147413, *11 (N.D. Cal., May 15, 2013), where the court concluded that “Plaintiffs here are not
 10 alleging that the products themselves are defective or injurious. Instead, Plaintiffs allege that Del
 11

12 ¹⁸ Indeed, the O’Neil declaration in no way contradicts Pirozzi’s allegations that she visited
 13 Apple’s website, which contained the misleading statements that the iPhone was safe and secure
 14 by design. Apple conveniently attempts to portray Pirozzi as a “casual user” but nothing in the
 15 CAC supports this contention. Instead, the screenshots attached to the declaration only serve to
 16 demonstrate that this advertisement was present on Apple’s website and could be viewed by
 17 prospective purchasers, like Pirozzi, who were trying to familiarize themselves with the iPhone
 before making a purchase of several hundred dollars. Moreover, the screenshots do not
 accurately portray how a user would view a website on his or her computer screen and should be
 further disregarded by the Court.

18 ¹⁹ Likewise, this exact argument was already rejected in Pirozzi II as untimely and should
 19 not be raised again given that the Court already sustained the action and found that Pirozzi met
 20 both Article III and CLRA, FAL, and UCL standing requirements. See Pirozzi II, 2013 4029067
 21 at *4-*9. Moreover, the case upon which Apple primarily relies, In re LinkedIn User Privacy
 22 Litig., 932 F. Supp. 2d 1089 (N.D. Cal. 2013) is furthermore readily distinguishable. In
 23 LinkedIn plaintiffs purchased premium access on a networking website that also offered free
 24 networking services. Id. at 1090. The website was hacked and plaintiffs’ password was posted
 25 on the internet. Id. Plaintiffs brought a claim alleging that they overpaid for the premium
 26 service. Id. The main drive for the court’s finding that plaintiffs did not meet Article III
 27 standing was that plaintiffs obtained premium membership for added networking capabilities, not
 28 for the added security for their passwords. Id. at 1093. This case is highly distinguishable.
 First, in LinkedIn, the website was hacked. Id. at 1090. LikendIn did not provided its partners
 with the ability to collect private information after telling consumers their information was safe –
 in fact, LinkedIn informed consumers that it could not provide “a 100% secure environment.”
Id. In contrast, here Plaintiffs alleged that they specifically purchased their iDevices because
 they expected that they will be able to download and use apps without compromising their
 personal and private information based on Apple’s own representations (CAC ¶¶ 9, 16-32, 121-
 27), but Apple then allowed its business partner app manufacturers to access and take private
 data (CAC ¶¶ 1-7, 107-20, 190, 212-14).

1 Monte has created misleading labeling and advertising for its products which fail to comply with
 2 objective FDA and Sherman Law standards. It is this misleading labeling and advertising that
 3 they allege caused them to purchase products or pay premiums they would not have otherwise,
 4 which meets Article III standing requirements.” Id. Other cases are in accord: Brazil v. Dole
 5 Food Co., 935 F. Supp. 2d 947, 961-62 (N.D. Cal. 2013) (allegations that, but for reliance upon
 6 mislabeling, plaintiff’s would not have purchased product sufficient to confer Article III
 7 Standing; plaintiff alleges that he and class members “spent money that, absent defendants’
 8 labeling, they would not have spent,” which constitutes “a quintessential injury-in-fact”);
 9 Bilodeau v. McAfee, Inc., 12-CV-04589, 2013 WL 3200658, *6 (N.D. Cal. June 24, 2013)
 10 (“because Plaintiff alleges that she ‘purchased a software product that is worth much less than
 11 what was reflected in the purchase price she paid’ as a result of Defendants’ respective
 12 misrepresentations, on its face, the complaint sufficiently alleges a concrete and particularized
 13 injury.”).²⁰

14 Here, Plaintiffs not only allege that Apple’s iDevices were defective, but further allege
 15 that Apple misled them *and* that as a result Plaintiffs’ personal data was misappropriated.
 16 Plaintiffs thus allege a specific harm they suffered which is causally related to Apple’s actions,
 17 which is all that is required for Article III standing.

18
 19
 20
 21
 22 ²⁰ See also Maya v. Centex, 658 F.3d 1060, 1069 (9th Cir. 2011) (Article III standing
 23 present where plaintiffs would not have purchased their homes absent defendants’
 24 misrepresentations); Delacruz v. Cytosport, Inc., 11-3532-CW, 2012 WL 1215243, * 8 (N.D.
 25 Cal. Apr. 11, 2012) (sufficient to allege reliance upon specific marketing materials claimed to be
 26 misleading for false advertising claims concerning the manner of marketing); Kwikset v.
 27 Superior Court, 51 Cal.4th 310, 329 (2011) (“for each consumer who relies on the truth and
 28 accuracy of a label and is deceived by misrepresentations into making a purchase, the economic
 harm is the same: the consumer has purchased a product that he or she paid more for than he or
 she otherwise might have been willing to pay if the product had been labeled accurately”); Cole
v. General Motors, 484 F.3d 717, 721-722 (5th Cir. 2007) (plaintiff’s actual economic harm
 (e.g., overpayment, loss in value, or loss of usefulness) emanating from the loss of their benefit
 of the bargain based on their purchase of a defective product sufficient for Article III – no injury
 or incurred remedial expense required).

1 **4. Non-California Plaintiffs Have Standing to Bring Claims Based on**
 2 **California Statutes**

3 Apple also argues that people who live outside of California have no standing to sue
 4 under various California laws, even where (as here) the activity that harmed them substantially
 5 emanated from California as a result of conduct by a California resident. This argument has no
 6 merit whatsoever.

7 The California Supreme Court’s decision in Sullivan v. Oracle Corp., 51 Cal. 4th 1191,
 8 1209 (2011), does not mandate dismissal of non-California residents’ consumer protection
 9 claims for lack of standing. Sullivan is a narrowly decided case involving a certified question
 10 from the Ninth Circuit concerning a wage dispute, and is therefore not apposite here. See
 11 Sullivan, 51 Cal. 4th at 1207; id. at 1209 (holding that UCL “does not apply . . . *in the*
 12 *circumstances of this case*” (emphasis added)). Indeed, given the limitation of the certified
 13 question procedure, the Court’s decision was narrow and it further distinguished two consumer
 14 class actions, because both cases (as here) involved fraudulent misrepresentations originating
 15 from California to induce a consumer transaction. See id. at 1208 n.10 (citing Wershba v. Apple
 16 Computer, Inc., 91 Cal. App. 4th 224 (2001) and Clothesrigger, Inc. v. GTE Corp., 191 Cal.
 17 App. 3d 605 (1987)).

18 To the contrary, in Wershba v. Apple Computer, Inc., the California Court of Appeal held
 19 that nationwide reach of California consumer law was appropriate where, as here, Apple was
 20 headquartered in California, class members were deceived by representations that were
 21 disseminated from California, substantial number of class members were located in California,
 22 and Apple’s decision-making occurred in California. Wershba, 91 Cal. App. 4th at 242. More
 23 recently, this Court rejected Apple’s very argument in another case, and found that consumers
 24 had standing to bring UCL, FAL and CLRA claims concerning Apple’s misrepresentations about
 25 the iPhone 4S, even though they were not California residents and did not purchase their iPhones
 26 in California:

27 Apple ‘conflate[s] two issues: the extraterritorial application of
 28 California consumer protection laws (or the ability of a nonresident
 plaintiff to assert a claim under California law), and choice-of-law
 analysis (or a determination that, based on policy reasons, non-
 forum law should apply).’ California courts have concluded that

1 'state statutory remedies may be invoked by out-of-state parties
 2 when they are harmed by wrongful conduct occurring in
 3 California.' Plaintiffs have alleged that their injuries were caused
 4 by Apple's wrongful conduct in false advertising that originated in
 5 California. Here, Plaintiffs have alleged that Apple's purportedly
 6 misleading marketing, promotional activities and literature were
 7 coordinated at, emanate from and are developed at its California
 8 headquarters, and that all 'critical decisions' regarding marketing
 9 and advertising were made within the state. . . . California's
 10 presumption against the extraterritorial application of its statutes
 11 therefore does not bar the claims of the out-of-state Plaintiffs,
 12 because this principle is 'one against an intent to encompass
 13 conduct occurring in a foreign jurisdiction in the prohibitions and
 14 remedies of a domestic statute.'

15 In re iPhone 4S Consumer Litig., 12-1127 CW, 2013 WL 3829653, *7 (N.D. Cal. July 23, 2013)

16 (internal citations omitted).

17 Apple's reliance on In re Apple & AT & T iPad Unlimited Data Plan Litig., 802 F. Supp.
 18 2d 1070, 1076 (N.D. Cal. 2011) is misplaced because in that case, AT&T's choice of law
 19 provision in its terms of service designates the law of each consumer's respective home state. Id.
 20 Here, as in iPhone 4S, "the alleged harmful conduct took place at least partially within
 21 California, and Apple does not argue that there is a choice of law provision that selects another
 22 state in any agreement between itself and consumers." iPhone 4S, 2013 WL 3829653, at *8. In
 23 fact, as of November 2009, Apple's online terms of service provide that "[y]ou agree that *all*
 24 *matters relating to your access to or use of the Site, including all disputes, will be governed by*
 25 *the laws of the United States and by the laws of the State of California* without regard to its
 26 conflicts of laws provisions. . . . and waive any objection to such jurisdiction or venue."
 27 (<http://www.apple.com/legal/internet-services/terms/site.html>) (emphasis added). Because
 28 Plaintiffs' consumer claims arise in part from Apple's marketing of the iDevices on its website,
 their claims are therefore governed by California law.

Apple's reliance on the Ninth Circuit decision in Mazza v. American Honda Motor Co.,
Inc., 666 F.3d 581 (9th Cir. 2012) is also misplaced. Indeed, the iPhone 4S court held that
Mazza does not support a finding that non-California residents lack standing to bring California
 consumer claims. iPhone 4S, 2013 WL 3829653, at *8 ("[I]n [Mazza], the court did not discuss
 whether the individual named plaintiffs may assert a claim against a defendant under California
 law. . . .[t]his case is currently at the pleading stage and '[w]hether or not certification on a

1 nationwide basis is appropriate in this case is not an issue that is currently before this Court.”);
 2 see also Donohue v. Apple, Inc., 871 F. Supp. 2d 913, 923 (N.D. Cal. 2012)
 3 (“Although *Mazza* may influence the decision whether to certify the proposed class and subclass,
 4 such a determination is premature” at the pleading stage). The court in Bruno v. Eckhart Corp.
 5 also rejected a similar argument and held that Mazza did not overrule the California Supreme
 6 Court’s decisions regarding the choice-of-law analysis required under California law, nor could
 7 it, because choice-of-law analysis is substantive state law and a state’s highest court is the final
 8 arbiter on state law. Bruno v. Eckhart Corp., 280 F.R.D. 540, 546 (C.D. Cal. Mar. 6, 2012)
 9 (citing Klaxon Co. v. Stentor Elec. Mfg. Co., 313 U.S. 487, 496 (1941); Fid. Union Trust Co. v.
 10 Field, 311 U.S. 169, 177-78 (1940)). Indeed, “Mazza did not vacate the district court’s class
 11 certification as a matter of law, but rather because defendant Honda met its burden to
 12 demonstrate material differences in state law and show that other states’ interests outweighed
 13 California’s.” In re POM Wonderful LLC Mktg. and Sales Practices Litig., 10-02199 DDP,
 14 2012 WL 4490860, *3 (C.D. Cal. Sept. 28, 2012) (finding that plaintiffs met their burden to
 15 show that California had sufficient contacts to the claims to ensure application of California law
 16 at class certification stage).

17
 18 **C. PLAINTIFFS’ MISREPRESENTATION CLAIMS AGAINST APPLE ARE PROPERLY
 PLED**

19 Apple seeks to dismiss what it labels Plaintiffs’ “misrepresentation” claims: their UCL
 20 claims (Counts 1 and 2), FAL claims (Counts 4 and 5), CLRA claims (Counts 6 and 7) and
 21 negligent misrepresentation claims (Counts 8 and 9). But all adequately state a claim and should
 22 not be dismissed.

23 **1. The Court Has *Already* Upheld These Claims**

24 Plaintiffs’ UCL, FAL, and CLRA and negligent misrepresentation counts are
 25 straightforward consumer protection claims. In fact, this Court has *already* upheld them. Pirozzi
 26 II, 2013 WL 4029067, at *3-*9. The CAC incorporates *verbatim* the following allegations (CAC
 27 ¶¶ 57-127) and claims against Apple from Pirozzi II: Count 1 (UCL), Count 4 (FAL), Count 6
 28 (CLRA) and Count 8 (negligent misrepresentation). With respect to Maria Pirozzi, the sole

1 representative plaintiff in the action Apple sought to dismiss in Pirozzi II, Apple makes no new
 2 arguments as to the inadequacy of her UCL, FAL and CLRA and negligent misrepresentation
 3 claims. There is no reason for the Court to revisit its previous decision, the reasoning and
 4 conclusions of which should be applied to uphold the other Plaintiffs' similar claims as well.

5 **2. Plaintiffs Have Met the Requirements of Rule 9(b)**

6
 7 Even assuming a heightened pleading requirement applies to Plaintiffs' UCL, FAL,
 8 CLRA and negligent misrepresentation claims,²¹ Plaintiffs have met their burden. While Rule
 9 9(b) requires that allegations of fraud be "specific enough to give defendants notice of the
 10 particular misconduct ... so that they can defend against the charge and not just deny that they
 11 have done anything wrong," Kearns v. Ford Motor Co., 567 F.3d 1120, 1124 (9th Cir. 2009), it
 12 does not require a plaintiff to catalogue every detail of his claims. See generally Cooper v.
 13 Pickett, 137 F.3d 616, 627 (9th Cir. 1997) ("we cannot make Rule 9(b) carry more weight than it
 14 was meant to bear" when analyzing pleading of securities claim).

15 In circumstances such as those found here, in which the complaint alleges a course of
 16 consistent but misleading statements by the defendant over an extended period of time, a plaintiff
 17 is not required "to allege, in detail, all facts supporting each and every instance of [fraud] over a
 18 multi-year period." Ticketmaster L.L.C. v. RMG Technologies, 07-2534ABCJCX, 2007 WL
 19 2989504, *2 (C.D. Cal. Oct. 12, 2007) (quoting U.S. ex rel. Lee v. SmithKline Beecham, Inc.,
 20 245 F.3d 1048, 1051-1052 (9th Cir. 2001)). To the contrary, when "a plaintiff alleges exposure
 21 to a long-term advertising campaign, the plaintiff is not required to plead with an unrealistic
 22 degree of specificity that the plaintiff relied on particular advertisements or statements." In re
 23 Tobacco II Cases, 46 Cal.4th 298, 328 (2009); see also Morgan v. AT & T Wireless Servs., Inc.,

24
 25 ²¹ Though Apple appears to contend that Plaintiffs' UCL, FAL, CLRA and negligent
 26 misrepresentation claims are all subject to Rule 9(b), that heightened pleading requirement
 27 applies only to allegations arising out of fraud. See, e.g., Goodman, 2012 WL 2412070, at *9
 28 (citing Vess v. Ciba-Geigy Corp. USA, 317 F.3d 1097, 1104 (9th Cir. 2003) (UCL claims under
 unfair and unlawful prongs not subject to Rule 9(b)); In re iPhone Application Litig., 844 F.
 Supp. 2d at 1072-1074 (applying Rule 9(b) to the fraudulent prong of the UCL, but not to the
 unfair or unlawful prong)).

1 177 Cal. App. 4th 1235, 1262 (2009) (“[W]here a fraud claim is based upon numerous
 2 misrepresentations, such as an advertising campaign that is alleged to be misleading, plaintiffs
 3 need not allege the specific advertisements the individual plaintiffs relied upon; it is sufficient for
 4 the plaintiff to provide a representative selection of the advertisements or other statements to
 5 indicate the language upon which the implied misrepresentations are based.”).

6 This Court has repeatedly taken a pragmatic approach when applying Rule 9(b)’s
 7 requirements to consumer claims. It may be impossible for consumers to remember the precise
 8 moment they are exposed to misrepresentations contained in advertisements and publicity
 9 campaigns, or to recall the exact language on which they relied — especially when the falsity of
 10 the statement comes to light years later. Thus, this Court has held it sufficient for a consumer to
 11 identify the “who” by identifying the manufacturer as the source of the statements, the “what” by
 12 identifying categories or types of misrepresentations, the “when” by identifying the general
 13 period of time over which the statements were made, the “where” by identifying the
 14 manufacturer’s website or other medium through which the statements were made, and the
 15 “how” by identifying why the statements were inaccurate and material. Clancy, 2013 WL
 16 4081632 at *10-*11.²² Other courts apply the Ninth Circuit standard in a similar manner. See,
 17 e.g., Lima v. Gateway, Inc., 710 F. Supp. 2d 1000, 1006 (C.D. Cal. 2010) (complaint satisfies
 18 Rule 9(b) when it alleged defendant as responsible for misrepresentations, “identifies the
 19 substance of the alleged misrepresentations” including some quotations, states the “time frame”
 20 of the statements as the period during which the product was sold until at least the date of
 21

22
 23 ²² This Court’s other cases cited in Clancy are also instructive. Astiana v. Ben & Jerry’s
 24 Homemade, Inc., 10–4387 PJH, 2011 WL 2111796, *6 (N.D. Cal. May 26, 2011) (“The ‘who’ is
 25 Ben & Jerry’s, Breyers, and Unilever. The ‘what’ is the statement that ice cream containing
 26 alkalized cocoa is ‘all natural.’ The ‘when’ is alleged as ‘since at least 2006,’ and ‘throughout the
 27 class period.’ The ‘where’ is on the ice cream package labels. The ‘how the statements were
 28 misleading’ is the allegation that defendants did not disclose that the alkalizing agent in the
 alkalized cocoa was potassium carbonate, which plaintiffs allege is a ‘synthetic.’); Chacanaca v.
Quaker Oats Co., 752 F. Supp. 2d 1111, 1126 (N.D. Cal. 2010) (upholding as sufficient
 allegations that “the particular statements they allege are misleading, the basis for that
 contention, where those statements appear on the product packaging, and the relevant time
 period in which the statements were used”).

1 plaintiffs' purchase, identifies the packaging, press releases and company websites as the
2 "where," and describes how the statements are false or misleading.)

3 Apple also contends that Plaintiffs failed to adequately allege reliance, but vastly
4 overstates the requirements for doing so. In re iPhone Application Litigation, 844 F. Supp. 2d at
5 1074, another Apple consumer case, is illustrative. The three paragraphs the Court deemed
6 adequate make only generic statements of reliance; stating that the plaintiffs "relied on Apple's
7 representations" that were material to their purchase (First Amended Consolidated Class Action
8 Complaint, Case No. 5:11-md-02250-LHK, Dkt. No. 25, ¶ 76); "relied upon and were deceived
9 by Apple's material misrepresentations and omissions regarding the iDevice (Id., ¶ 320); and
10 "reasonably relied on Apple's representations" (Id., ¶ 329). The Court found through those three
11 terse statements, "Plaintiffs have adequately alleged that they relied upon Apple's
12 representations." In re iPhone Application Litigation, 844 F. Supp. 2d at 1074 ("While a
13 plaintiff must show that the misrepresentation was an immediate cause of the injury-producing
14 conduct, the plaintiff need not demonstrate it was the only cause." (citing In re Tobacco II Cases,
15 46 Cal.4th at 326–27)). Here, Plaintiffs have also met that minimal burden.

16 17 **3. The CAC Details Apple's False and Misleading Statements**

18 The CAC describes in detail a long course of false and misleading statements relating to
19 the privacy of its iDevices. Those allegations include (1) general descriptions of Apple's
20 misrepresentations, (2) particularized descriptions of the contents of specific misrepresentations,
21 and (3) quotation from certain false and misleading statements. For example:

- 22
- 23 • "Apple has repeatedly represented that Apple's products are safe and secure, and
24 that private information could not be accessed by third-party apps without the
25 user's express consent." (CAC ¶ 64.)
- 26 • Apple has represented to Plaintiffs and other purchasers, expressly or by
27 implication, that iDevices are "[s]afe and secure" and that "iOS4 is highly secure
28 from the moment you turn on your iPhone. All apps run in a safe environment, so

1 a website or app can't access data from other apps.²³ iOS 4 supports encrypted
 2 network communication to protect your sensitive information. ... To guard your
 3 privacy, apps requesting location information must get your permission first.”
 4 (CAC ¶ 123 (quoting Apple website as of September 2011), CAC ¶ 102²⁴.)

- 5 • “Since 2010, App Store’s guidelines provided that ‘Apps cannot transmit data
 6 about a user without obtaining the user’s prior permission and providing the user
 7 with access to information about how and where the data will be used.’ The
 8 guidelines further provided that ‘Apps that require users to share personal
 9 information, such as email address and date of birth, in order to function will be
 10 rejected.’” (CAC ¶ 104.)
- 11 • “In February 2012, an Apple spokesperson, Tom Neumayr, further reaffirmed that
 12 ‘apps that collect or transmit a user’s data without their permission are in
 13 violation of our guidelines.’” (CAC ¶ 106.)
- 14 • “Apple has represented to Plaintiffs and other purchasers, expressly or by
 15 implication, that the App Store does not permit apps that ‘violate[] [Apple’s]
 16 developer guidelines including apps that violate user privacy.’” (CAC ¶ 121.)
- 17 • “Apple has represented to Plaintiffs and other purchasers, expressly or by
 18 implication, that ‘Apple takes precautions – including administrative, technical,
 19 and physical measures – to safeguard [purchaser’s] personal information against
 20 loss, theft, and misuse, as well as against unauthorized access, disclosure,
 21 alteration, and destruction.’” (CAC ¶ 122 (quoting Apple’s privacy policy).)
- 22 • “Apple also assured consumers that for data-security purposes, ‘Applications on
 23 the device are “sandboxed” so they cannot access data stored by other
 24 applications.’ Apple, in its iDevice literature, identifies the “Contacts” feature as
 25 such an ‘application.’” (CAC ¶ 209 (quoting Apple publication, “Deploying
 26 iPhone and iPad, Security Overview”).)
- 27 • “Apple ... acts as a gatekeeper to the App Store. Indeed, when Apple first
 28 launched the App Store [in July 2008], Steve Jobs stated, ‘[t]here are going to be
 some apps that we’re not going to distribute. Porn, malicious apps, *apps that
 invade your privacy.*’” (CAC ¶ 92 (emphasis added).)

23 ²³ Apple claims that its description of iOS is not false because “iOS4 was designed to
 24 prevent apps (e.g., Twitter) from accessing data from other apps (e.g., Facebook)” but that the
 25 statement “makes no claim that apps cannot access data stored *by the user in iOS*, such as
 26 calendar or contact information.” (Apple MTD at 6.) Apple’s position that Contacts is not an
 27 “app” is a nicety certain to be lost on consumers. The icon for Contacts is displayed on the
 28 iDevice screen just like that for Facebook or Twitter, and Apple itself has used the term “app” to
 refer to Contacts. In any event, this just raises a fact question.

²⁴ CAC at paragraph 103 alleges that Apple makes similar claims about the iPad and iPod
 Touch.

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24
- 25
- 26
- 27
- 28
- “In October 2007 Jobs similarly stated: ... ‘[We’re trying to] protect iPhone users from viruses, malware, *privacy attacks*, etc.’” (CAC ¶ 94 (emphasis added).)
 - “Likewise, Jobs, who often responds to users emails, wrote in a much publicized email responding to a reporter’s question: ‘Yep, freedom from programs that steal your private data’” (CAC ¶ 96.)
 - “Apple has represented to Plaintiffs and other purchasers, expressly or by implication, that: ‘Apple takes precautions - including administrative, technical, and physical measures - to safeguard your personal information against loss, theft, and misuse, as well as against unauthorized access, disclosure, alteration, and destruction.’ *See e.g.*, Apple’s customer privacy policy.” (CAC ¶ 122.)
 - Apple has represented to Plaintiffs and other purchasers, expressly or by implication, that iDevices are “[s]afe and secure” and that “iOS 4 is highly secure from the moment you turn on your iPhone. All apps run in a safe environment, so a website or app can’t access data from other apps. iOS 4 supports encrypted network communication to protect your sensitive information... To guard your privacy, apps requesting location information must get your permission first.” “However, third-party apps such as Hipster and Path have admittedly accessed and uploaded users’ full contacts information without user consent. Likewise, the iDevices are vulnerable to third-party apps uploading photos and videos when requesting access to user’s location, despite Apple’s promise that the iOS is secure and that apps cannot access data from other apps.” (CAC ¶ 123.)
 - After the issues that form the basis for this lawsuit came to light, Apple reiterated that “Apps that collect or transmit a user’s contact data without their prior permission are in violation of [Apple’s] guidelines.” (CAC ¶ 137.)
 - “From 2008 to the present, the highest levels of Apple (from its founder to its current CEO to its corporate spokespersons) have so consistently expressed publicly that Apple protects its customers’ and iDevice owners’ security and privacy that – though inaccurate – it is ingrained into the image of Apple’s culture, products and offerings as well as in the minds of customers. Apple has never corrected this falsity or misimpression.” (CAC ¶ 211.)
 - “Specifically, as described herein, Apple has made the following representations, expressly or by implication, to Plaintiffs and other members of the Class about the iDevices: (i) that Apple designed the iDevices to safely and reliably download third party apps, (ii) that the App Store does not permit apps that violate its developer guidelines (including apps that contain pornography, violate user privacy, and hog bandwidth) to be sold or to be made available for free through the App Store, (iii) that ‘Apple takes precautions – including administrative, technical, and physical measures – to safeguard [purchaser’s] personal information against loss, theft, and misuse, as well as against unauthorized access, disclosure, alteration, and destruction’; (iv) that Apple does not allow one app to access data stored by another app; and (v) that Apple does not allow an app to transmit/upload/download data from iDevices without the user’s consent.” (CAC ¶ 511.)

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- “Apple represented that the iDevices and Apple’s associated services have characteristics, uses and benefits they do not have; were of a particular standard, quality and grade, but were in fact not; that they had been supplied in accordance with previous representations when they had not; and in that Apple advertised and sold iDevices with the intent not to sell them as advertised. In particular, Apple falsely represented that iDevices were highly secure, ‘sandboxed,’ and accompanied by a fully functioning App Store with immediate access to Apps, that the add-on component Apps available in the App Store were not harmful, malicious or violative of user privacy, that the App Store was appropriately curated, and that Apple would not allow malicious Apps or Apps that invade iDevice owner’s privacy to be available via the App Store.” (CAC ¶ 520.)

8

9 The CAC also alleges that Plaintiffs relied on Apple’s misrepresentations. For example:

- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24
- “Plaintiffs purchased their iDevices with the expectation that Apple designed the iDevices to protect user privacy and would not have purchased their iDevices and/or would have paid less for the iDevices had they known the truth about the iDevices. Instead, Plaintiffs have learned that third-party apps are capable of accessing private user data such as users’ photos, videos, and contacts without user consent. Plaintiffs allege that Apple designed the iDevices in such a way as to make these devices vulnerable to unauthorized access by third-parties, despite their misrepresentations that such access was impossible. Apple’s failure to disclose that third-party apps had the ability to access private photo and contact information resulted in harm to Plaintiffs and the Class. Plaintiffs purchased their iDevices with the expectation that their private information would remain safe and would not have paid as much for their iDevices if they knew that Apple did not properly safeguard these devices.” (CAC ¶ 64.)
 - “Plaintiffs and members of the Class relied upon Apple’s representations with respect to the cost of their iDevices when making their purchasing decisions, and the omission of material facts to the contrary was an important factor in their decision.” (CAC ¶ 124.)
 - “For example, Plaintiff Pirozzi viewed the Apple website and saw in-store advertisements prior to purchasing her iPhone.” (CAC ¶ 125.)
 - “Likewise, each of the other Plaintiffs visited Apple’s website, saw in-store advertisements, and/or was aware of Apple’s representations regarding the safety and security of the iDevices prior to purchasing their own iDevices.” (CAC ¶ 126.)

25 As the Court held in Pirozzi II, those allegations sufficiently set out the facts with the

26 required specificity. Pirozzi II, 2013 WL 4029067 at *6-*7. The CAC states the “who” (Apple)

27 (CAC ¶¶ 1-9, 11); the “what” (that Apple made specific representations that it protects user

28 privacy, that it does not allow malicious apps into the app store, and that Apple’s operating

1 system is secure and that apps cannot transmit user data without user’s prior consent) (CAC ¶¶
 2 80-82, 121-127); the “when” (from 2008 to the present, Apple made repeated representations
 3 that it is responsible for user experience and will not allow malicious apps) (CAC ¶¶ 64, 80-82,
 4 87-99); the “where” (the Apple website, App Store, privacy policy, and guidelines) (CAC ¶¶
 5 121-126); and the “how” (Apple knew or should have known that the Apple Devices were not
 6 secure and that apps were accessing and uploading user data) (CAC ¶¶ 107-120).

7 8 **4. Apple’s Arguments Are Unavailing**

9 Apple contends that those allegations are insufficient because they do not detail when
 10 each individual saw or heard each individual misrepresentation. However, that minute
 11 specificity is not required. Tobacco II, 46 Cal. 4th at 327 (“Nor does a plaintiff need to
 12 demonstrate individualized reliance on specific misrepresentations to satisfy the reliance
 13 requirement.”).

14 Apple’s motion attempts to draw parallels to a line of cases in which the plaintiff plainly
 15 failed to plead *any* reliance on the alleged misstatements. In four of the cases, the complaint
 16 failed because it did not include any contention that any plaintiff looked at the website
 17 containing the misrepresentation in question. Delacruz v. Cytosport, Inc., C 11-3532 CW, 2012
 18 WL 1215243, *9 (N.D. Cal. Apr. 11, 2012) (“Plaintiff ... does not plead that she read or relied
 19 on any statements on the website.”); Durell v. Sharp Healthcare, 183 Cal. App. 4th 1350, 1363
 20 (2010) (“The SAC does not allege Durell relied on ... Sharp’s Web site representations....
 21 Indeed, the SAC does not allege Durell ever visited Sharp’s Web site....”); Gitson v. Trader
 22 Joe’s Co., C 13-cv-01333 WHO, 2013 WL 5513711, *6 (N.D. Cal. Oct. 4, 2013) (complaint did
 23 “not allege that the plaintiffs ever saw Trader Joe’s website or what the website states”); Garcia
 24 v. Sony Computer Entm’t Am., LLC, 859 F. Supp. 2d 1056, 1063 (N.D. Cal. 2012) (dismissal
 25 based on a failure to plead any reliance or knowledge of the website misstatements). In another,
 26 Bruton v. Gerber Prods. Co., C 12-CV-2412 LHK, 2013 WL 4833413, *16 (N.D. Cal. Sept. 6,
 27 2013), the plaintiff similarly failed to allege that she had seen the website in question, but
 28 attempted to allege constructive knowledge based on an incorporation by reference theory, which

1 the Court rejected. Similarly, In re Google Android Consumer Privacy Litig., 11-MD-02264
2 JSW, 2013 WL 1283236, *6 (N.D. Cal. Mar. 26, 2013) and Kane v. Chobani, Inc., C 12-2425
3 LHK, 2013 WL 5289253, *9 (N.D. Cal. Sep. 19, 2013) each involved an absence of allegations
4 of exposure to or reliance on the alleged misrepresentations. In Baba v. Hewlett-Packard Co., C
5 09-05946 RS, 2010 WL 2486353, *5 (N.D. Cal. June 16, 2010), plaintiffs appear to have pled
6 reliance on their expectation that “HP would honor its warranty” but no allegations of reliance on
7 the alleged misrepresentations themselves.

8 None of those cases is analogous to the situation here. Though Apple focuses on one
9 statement contained on its website, the complaint is replete with specific and general allegations
10 detailing a long course of misrepresentations by the company. Even with respect to the website
11 statement, the CAC specifically states that three plaintiffs learned of Apple’s misrepresentations
12 by visiting the company’s website.²⁵ (CAC ¶¶ 24, 28, 31.) There is no requirement that a
13 consumer reconstruct distant history and identify the exact date on which they accessed a
14 particular URL on Apple’s website. In that regard, Apple’s factual contention that the website is
15 voluminous, containing “thousands of individual webpages that are continually updated,”
16 underscores the absurdity of the standard it would have the Court adopt. (O’Neil Decl. ¶10.) It
17 would be logistically impossible for a consumer to go back and identify where Apple parked the
18 particular webpage on a given day many years back. The task may be impossible for even
19 Apple, whose submission to the Court uses a third-party archive (the Wayback Machine) to
20 identify historical versions of its own site. A consumer should not waive claims because he or
21 she is unable to pinpoint the exact series of links used to access a page containing a false or
22 misleading statement.

23 _____
24 ²⁵ Apple places heavy emphasis on its factual contention that it says shows that two of the
25 representative plaintiffs, Hoffman and Varner, purchased their iPhones and downloaded certain
26 defendants’ apps prior to the date Apple says one of its misrepresentations was posted on its
27 website. The accuracy of Apple’s declaration and records cannot be verified without discovery,
28 but in any event the submission does not affect the outcome of any part of its motion. Plaintiffs
have alleged a continuing pattern of consistent misrepresentations, and the possibility that two of
them may misremember which specific similar misrepresentation they saw does not change their
claim, much less deprive Apple of sufficient information to defend the lawsuit. If anything, such
a factual error — even if proven — underscores the policy behind not requiring Plaintiffs to
identify which specific statement in a pattern of misrepresentations they relied on.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

5. Class Claims Based on Misrepresentations the Class Representatives Did Not See May Be Maintained

The CAC adequately contends that each of the plaintiffs learned of Apple's misrepresentations from Apple's website or from in-store advertising or other means (CAC ¶¶ 24, 28, 31, 126), including, for certain plaintiffs, "store, print and television ads concerning the products" (CAC ¶¶ 19, 24, 28, 31), and "watch[ing] numerous live blogs and web announcements," including those led by Steve Jobs (CAC ¶¶ 24, 31). That is sufficient under Tobacco II. Moreover, in the class action context, a plaintiff has broader latitude to stand in for class members who may have heard different but consistent misrepresentations by the defendant. There is no requirement that *each* plaintiff have viewed *each* misrepresentation, or even that each misrepresentation have been relied on by at least one of the representatives. As the Court recently held in Clancy, so long as standing is established, the question of whether the plaintiff may maintain class claims based on statements he did not hear is a question for class certification, not a motion to dismiss. Clancy, 2013 WL 4081632 at *5. The same result was reached in Cardenas v. NBTY, Inc., 870 F. Supp. 2d 984, 992 (E.D. Cal. 2012), where, after reviewing the relevant authorities, the court concluded that the issue is not one of standing but of typicality and adequacy of representation. Id. (citing Bruno v. Quten Research Inst., LLC, 280 F.R.D. 524, 530 (C.D. Cal. 2011) (saying the "treatises and the vast majority of persuasive authority" agree); see also Koehler v. Litehouse, Inc., CV 12-04055 SI, 2012 WL 6217635, *5 (N.D. Cal. Dec. 13, 2012). Therefore, Apple's contention that the absence of contentions connecting certain plaintiffs with specific misrepresentations is of little import here. As long as the Plaintiffs have adequate standing, which they do, they are able to maintain claims based on allegations of a broad array of misrepresentations at the pleading stage.

25
26
27
28

6. Apple's Material Omissions Give Rise to Liability

Plaintiffs have also pled an independent basis for their CLRA, FAL and UCL claims: Apple's failure to disclose material facts. For example, the CAC alleges that though "Apple ... repeatedly represented that Apple's products are safe and secure, and that private information

1 could not be accessed by third party apps without the user’s consent ... Apple designed the
 2 iDevices in such a way as to make these devices vulnerable to unauthorized access by third
 3 parties, despite their misrepresentations that such access was impossible. Apple’s failure to
 4 disclose that third party apps had the ability to access private photo and contact information
 5 resulted in harm to Plaintiffs and the class.” (CAC ¶ 64.) The CAC also alleges that “Apple
 6 never disclosed to Plaintiffs that their iDevices would or could ... self-transmit the iDevice
 7 address book without user input or authorization from the iDevice owner,” though it “knew of
 8 the security hole and of episodic, App-initiated exploitations of this iDevice flaw for some time.”
 9 (CAC ¶¶ 215–16.) Plaintiffs contend that the omissions give rise to liability under the UCL:
 10 “Apple had a duty to disclose the material privacy and security characteristics of the iDevices
 11 and their operations” because it knew or should have known of the problems, “had exclusive
 12 knowledge of material facts that were not known to Plaintiffs,” and “made representations
 13 regarding the iDevices’ protection of user privacy without disclosing that iDevices were not safe
 14 and that apps were capable of accessing private user data without consent” (CAC ¶ 457); and
 15 “Apple had a duty to disclose” that information because it knew or should have known the
 16 information, because it “had exclusive knowledge of [those] material facts that were not known
 17 to Plaintiffs,” and because it “made representations regarding the iDevices’ features
 18 accompanying an iDevice purchase” that contradicted the material facts known to Apple. (CAC
 19 ¶ 471.) They also allege that Apple’s nondisclosures as one of the bases for their FAL claim
 20 (CAC ¶¶ 496–498) and CLRA claim (CAC ¶¶ 507–529²⁶).

21 Under California law:

22 A failure to disclose a fact can constitute actionable fraud or deceit
 23 in four circumstances: (1) when the defendant is the plaintiff’s
 24 fiduciary; (2) when the defendant has exclusive knowledge of

25 _____
 26 ²⁶ Plaintiffs’ direct CLRA claims (Counts VI and VIII) incorporate by reference the specific
 27 preceding allegations concerning Apple’s material omissions. To the degree any additional
 28 specificity is required, amendment would be accomplished merely by addition of the generally
 pled allegations to the specific CLRA counts. Though Plaintiffs request leave to so amend if
 necessary, Apple cannot claim confusion about Plaintiffs’ claims and the ministerial task of
 amendment should not be required.

1 material facts not known or reasonably accessible to the plaintiff;
 2 (3) when the defendant actively conceals a material fact from the
 3 plaintiff; and (4) when the defendant makes partial representations
 that are misleading because some other material fact has not been
 disclosed.

4 Collins, 202 Cal. App. 4th 249, 255-56 (2011) (citing LiMandri v. Judkins, 52 Cal. App. 4th 326,
 5 336 (1997); Falk v. General Motors Corp., 496 F. Supp. 2d 1088, 1094–95 (N.D. Cal. 2007)).

6 The CAC pleads three of the four bases applicable here: (a) Apple’s exclusive knowledge (CAC
 7 ¶ 457), (b) active concealment (CAC ¶¶ 467(g), 759) and (c) Apple’s misleading statements and
 8 misrepresentations.

9 Apple lodges three defenses to Plaintiffs’ material omission claims.²⁷ First, Apple
 10 contends that the CDA provides immunity to “an interactive computer service like Apple” for a
 11 “fail[ure] to provide sufficient warnings about potential risk associated with third-party content
 12 available on its platforms.” (Apple MTD at 29.) As discussed above, Apple is not entitled to the
 13 benefit of CDA immunity at all. Moreover, Apple misconstrues Plaintiffs’ material omission
 14 claims, which are not limited to a failure to warn about what *third parties* might do, but directly
 15 allege that *Apple* failed to warn about a flaw in *its own* iDevices. (CAC ¶ 64 (“Apple designed
 16 the iDevices in such a way as to make these devices vulnerable ...”); and ¶ 215 (“Apple never
 17 disclosed to Plaintiffs that their *iDevices* would or could ... self-transmit the iDevice address
 18 book” without consent) (emphasis added).) CDA immunity simply does not cover claims against
 19 a hardware manufacturer arising out of flaws in that manufacturer’s own products.

20 Second, Apple contends that “absent an affirmative misrepresentation, a manufacturer is
 21 not liable for a failure to disclose a latent defect except in situations posing an ‘unreasonable
 22 safety hazard.’” (Apple MTD at 29, quoting Wilson v. Hewlett-Packard Co., 668 F.3d 1136,
 23 1141–43 (9th Cir. 2012).) The factual predicate for that argument is faulty—as detailed above,
 24

25 ²⁷ Apple does not appear to argue a failure to plead reliance on the omissions, nor could it.
 26 To demonstrate reliance on an omission, “[o]ne need only prove that, had the omitted
 27 information been disclosed, one would have been aware of it and behaved differently.” Mirkin
 28 v. Wasserman, 5 Cal. 4th 1082, 1093 (1993). “[A] presumption of reliance is appropriate in
 cases alleging omissions.” Overton v. Bird Brain, Inc., 11-1054, 2012 WL 909295, *5 (C.D.
 Cal. Mar. 15, 2012).

1 Plaintiffs *have* repeatedly alleged multiple misrepresentations by Apple. Those statements
 2 constitute much more than mere “partial misrepresentations” necessary to impose an affirmative
 3 duty to make a corrective disclosure of known material facts.²⁸ But Apple also misconstrues the
 4 “safety concern” limitation discussed in Wilson. California law does not limit material omission
 5 claims to situations involving unreasonable safety defects, *except* when the alleged omission
 6 relates to a defect that manifests *outside* the warranty period. Keegan v. Am. Honda Motor Co.,
 7 Inc., 284 F.R.D. 504, 529 (C.D. Cal. 2012) (“If a claim based on a failure to disclose arises
 8 outside the warranty period, the undisclosed defect must pose ‘safety concerns.’”).²⁹

9 California cases post-dating Wilson have reiterated the rule that the “safety concern”
 10 limitation applies only to claims that arise exclusively after the warranty period. In Collins, the
 11 Court of Appeal explained that California’s narrowing of post-warranty material omission claims
 12 was based on a concern that allowing such claims would “supplant warranty law,” meaning that
 13 the “failure of a product to last forever would become a ‘defect’” preventing a manufacturer
 14 from issuing limited warranties. Collins, 202 Cal. App. 4th at 256–57. Examining the primary
 15 authorities on which Wilson relies, Daugherty v. American Honda Motor Co., Inc., 144 Cal.
 16 App. 4th 824 (2006) and Bardin v. Daimlerchrysler Corp., 136 Cal. App. 4th 1255 (2006), the
 17 Collins court explained that material omission claims that arose *during* the warranty period were
 18 not narrowed. Plaintiffs’ claims in Collins involved the manufacturer’s failure to disclose a
 19 problem with the controller for a computer floppy disk—an issue “central to the function of a
 20

21
 22 ²⁸ California law contains no requirement that a plaintiff have known of, or relied on, the
 23 original statement. Such a requirement would eliminate any difference between the affirmative
 24 duty to speak and a prohibition on the original misstatement.

25 ²⁹ In Wilson itself, the Ninth Circuit recognized that material omission claims were limited
 26 to issues giving rise to “safety concerns” only when the alleged defect arose only outside the
 27 warranty period. It distinguished two cases: Tietsworth v. Sears, Roebuck & Co., 720 F. Supp.
 28 2d 1123 (N.D. Cal. 2010), stating that “the plaintiffs in that case alleged that they began
 experiencing problems ‘within the first months of purchasing the Machine’—*i.e.*, *within* the
 express warranty period,” Wilson, 668 F.3d at 1142 n. 1 (emphasis in the original, citation
 omitted), and Baba, 2010 WL 2486353, at *3-*4, because in that case, “the defect manifested
 during the express warranty period, and is thus distinguishable from the present case.” Wilson,
 668 F.3d at 1143.

1 computer as a computer” but plainly not a safety concern. Nevertheless, the court upheld the
 2 claims, holding that because the problem arose immediately upon purchase, the claims did not
 3 “attempt an end run around the warranty laws.” Id. at 257.

4 Apple fails to cite that authority, or the case in which this Court ruled against it on the
 5 *exact same issue*. In Donohue v. Apple, Inc., 871 F. Supp. 2d at 926–27, plaintiffs brought
 6 material omission claims, based on “exclusive knowledge,” and “active concealment” theories,
 7 relating to a problem with the signal meter in some of the same iDevices at issue here. Id. at
 8 926. There, Apple argued that the claims were barred by Wilson and Vitt v. Apple Computer,
 9 Inc., 469 Fed. Appx. 605 (9th Cir. 2012), the only other case it cites here. The Court rejected
 10 those contentions, and distinguished Apple’s authorities, finding them limited to claims arising
 11 only after the warranty period and rooted in the concern that allowing such claims would
 12 “eliminate term limits on warranties.” Donohue, 871 F. Supp. 2d at 926 (citations omitted).

13 By contrast, plaintiff here alleges that his iPhone failed to perform
 14 from the moment he purchased it. The case therefore does not
 15 raise similar policy concerns regarding potential conflicts between
 16 a manufacturer’s right to limit its liability under warranty and its
 duty to disclose known defects. Consequently, the court finds
 Apple’s authorities materially distinguishable.

17 Id. (citing Baba, 2010 WL 2486353, at *4 (finding inapposite cases that “involved alleged
 18 defects that had manifested themselves after expiration of the warranty period”)). The same
 19 reasoning should be applied, and the same result reached, here.

20 Finally, Apple claims that its Privacy Policy did disclose that iPhone apps “*may* collect
 21 information including “such things as location data or contact details.” A generalized statement
 22 that in certain circumstances certain applications may, with disclosure and consent, gather certain
 23 unspecified “contact details,” is facially insufficient to correct a long campaign of misstatements,
 24 especially in light of Apple’s actual knowledge that such privacy was accessible without consent
 25 and was repeatedly been accessed without consent. At a minimum, Apple’s defenses are highly
 26 factual and cannot be resolved at the pleading stage.³⁰

27
 28 ³⁰ Apple cites three readily distinguishable cases. In Fabozzi v. StubHub, Inc., C 11-4385
 EMC, 2012 WL 506330, *6 (N.D. Cal. Feb. 15, 2012), the plaintiff conceded the fraud-based
 UCL claim at issue, based on the defendant’s unambiguous, repeated, prominent disclosures of
 Case No. : 13-cv-00453-JST -40- OPP’N TO APPLE MOT. TO DISMISS

1
2 **D. PLAINTIFFS' OTHER CLAIMS ARE ALL PROPERLY PLED**

3 a) *California Computer Crime Law, Cal. Penal Code § 502*

4 Plaintiffs' CAC alleges that Apple violated California Penal Code §§502(c)(1),(2), and
5 (6-8). (CAC ¶¶ 539-569.) These sections, which generally address computer-related crimes,
6 also impose civil liability upon any person who:

7 (1) knowingly accesses and without permission alters, damages, deletes,
8 destroys or otherwise uses any data, computer system, or computer
9 network in order to either (a) devise or execute a scheme or artifice to
defraud, deceive or extort or (b) wrongfully obtain money, property or
data, §502(c)(1) (emphasis added);

10 (2) knowingly accesses and without permission takes, copies or makes use
11 of any data from a computer, computer system, or computer network, or
12 takes or copies any supporting documentation, whether existing or
residing internal or external to a computer, computer system or computer
network, §502 (c)(2) (emphasis added);

13 (3) knowingly and without permission provides or assists in providing a
14 means of accessing a computer, computer system, or computer network in
violation of this section, 502(c)(6);

15 (4) knowingly and without permission accesses or causes to be accessed
16 any computer, computer system or computer network, §502 (c)(7); or

17 (5) knowingly introduces any computer contaminant into any computer,
18 computer system or computer network, §502(c)(8) (emphasis added).

19 Apple violated several of these clauses and Plaintiffs' pleadings satisfy these claims. (Id.)
20 Apple does not deny this. Instead, Apple argues: (1) that it did not "introduce" the Apps because
21 Plaintiffs downloaded them from Apple's App Store, (2) Apple had permission because plaintiffs

22
23 the allegedly undisclosed fact at the time of the transactions at issue. In Janda v. T-Mobile,
24 USA, Inc., C 05-03729, 2009 WL 667206, *6 (N.D. Cal. Mar. 13, 2009), aff'd 378 F.Appx. 705
25 (9th Cir. 2010), the claim was based on an alleged failure to disclose that a statement that the
26 price monthly service price "excludes taxes and surcharges" somehow omitted the possibility
27 that additional taxes and surcharges might be added. The implausible claims made by the
28 plaintiffs in those cases differed radically from those pled here. Finally, Birdsong v. Apple, 590
F.3d 955, 961 (9th Cir. 2009) involved an alleged risk of hearing loss due to use of the Apple
iPod. The referenced section rejects plaintiffs' "benefit of the bargain" theory on the basis that
Apple made no promises about the auditory safety of its products and warned against high
volumes. Id. It has no applicability to the issue for which it is cited.

1 downloaded the Apps, and (3) Plaintiffs suffered no damage. None of these arguments have
2 merit.

3 Apple's simplistic assertion that Plaintiffs downloaded apps to their iDevices begs the
4 question: Plaintiffs did not know that the apps contained the malicious code at issue here. (CAC
5 ¶ 62.) Plaintiffs also were forced to use the App store for any software as a result of Apple's
6 controls over iDevices. (CAC ¶ 60.) These circumstances do not create "permission" for Apple
7 and the App Defendants to take Plaintiffs' personal data, such as their Contacts, without
8 permission and in violation of Apple's purported policies and public statements.

9 As for Apple's one sentence assertion claim that no damage occurred, as discussed
10 above, damage did occur and Plaintiffs were harmed.

11
12 *b) Conversion*

13 Plaintiffs' CAC sufficiently alleges conversion by Apple. The elements of conversion
14 are (1) plaintiff owns, legally possesses, or is entitled to possess certain property; and (2) the
15 defendant unlawfully and without authorization assumed and exercised dominion and control
16 over the property in a manner inconsistent with the plaintiff's rights.³¹ Here, Plaintiffs own their
17 iDevice personal data and Contacts, which have intrinsic and commercial value. (CAC ¶¶ 151,
18 162-171, 205.) The Defendants uploaded this personal data without authorization, thereby
19 acquiring them wrongfully, unlawfully and in a manner that invaded Plaintiffs' privacy. (CAC
20 ¶¶ 142-44, 148, 151, 160, 162-171, 238-245, 259, 262-267, 282-283, 290-292, 301-307, 314-
21 322, 325, 329-333, 341, 345-346, 349-352, 355-358, 361-364, 371-377, 388-400, 409, 428-430,
22 629-633, 649.) Plaintiffs' therefore allege a cognizable conversion claim against Apple.

23 Nevertheless, Apple seeks dismissal of the claim on two grounds. First, it argues that
24 while the App Defendants may have converted Plaintiffs' property, it did not. Second, it

25
26
27 ³¹ Hunt v. Baldwin, 68 S.W.3d 117, 131 (Tex. 2001); Horton v. Jack, 126 Cal. 521, 526
28 (1899). Plaintiffs' CAC satisfies this standard. Where, like Defendants did here, a party acquires
the property wrongfully, demand for the property's return is not necessary to establish the tort of
conversion. See Presley v. Cooper, 284 S.W.2d 138, 141 (1955).

1 suggests that there can be no conversion because Plaintiffs did not lose access to their data. Both
2 arguments fail.

3 As alleged throughout the CAC, Apple acted hand in glove with the App Defendants to
4 develop and distribute the malfeasant apps. (CAC ¶¶ 3, 61-63, 87, 107.) As such, Apple
5 participated in, and did convert Plaintiffs' personal data.

6 Further, conversion does not require that Plaintiffs lose all copies of the stolen data.
7 Once a copy was made, Plaintiffs lost control over *that copy*. That is sufficient to state a claim
8 for conversion. Otherwise, it would be impossible to convert electronic data unless one
9 destroyed the data after taking it.

10
11 *c) Trespass to Chattels*

12 Apple also simply misunderstands this claim, as shown by its odd argument that it does
13 not cover electromagnetic intrusion onto land. Under Texas law, the wrongful interference with
14 the use or possession of another's property constitutes actionable trespass. Omnibus Int'l, Inc. v.
15 AT&T, Inc., 111 S.W.3d 818, 826 (Tex. 2003). While the commission of a trespass does not
16 necessarily subject a defendant to liability for damages, liability does attach when there are
17 actual damages to the property or the owner is deprived of its use for a substantial period of time.
18 Zapata v. Ford Motor Credit Co., 615 S.W.2d 198, 201 (Tex. 1981). Similarly, under California
19 law, trespass to chattels lies where an intentional interference with the possession of personal
20 property has proximately caused injury. Intel v. Hamidi, 30 Cal.4th 1342, 1350-51 (2003).

21 Here, Apple, in concert with the App Defendants, wrongfully interfered with and used
22 Plaintiffs' tangible property (their iDevices) and Plaintiffs' intangible property (their iDevice
23 personal data, including their Contacts). As such, Plaintiffs allege viable trespass claims under
24 Texas and California law. (CAC ¶¶ 7, 135, 147-151, 428-433, 652, 662-671.)

25 More particularly, Defendants, without Plaintiffs' consent, placed malware on Plaintiffs'
26 iDevices, which made those iDevices initiate "calls" and enabled Defendants to unlawfully spy
27 on Plaintiffs and acquire Plaintiffs' personal data. (Id.) Defendants also captured and
28 disseminated Plaintiffs' iDevice address books to unauthorized recipients and servers via the

1 internet. (Id.) Defendants therefore not only made Plaintiffs' iDevice function counter to
 2 Plaintiffs' intent, they did this secretly, without Plaintiffs' consent, and unjustly benefitted and
 3 profited at Plaintiffs' detriment and expense. (Id.)

4 Defendants' conduct impaired the functioning of Plaintiffs' iDevices and interfered in a
 5 tangible, real way with the operations of their iDevices and the Contacts and other personal data
 6 thereon. (CAC ¶¶ 428, 652, 662-671.) Their conduct also depleted the users' iDevice battery
 7 life and resources like memory and energy, lessened the actual life of the device and transformed
 8 their Contacts from a constitutionally protected list solely controlled by Plaintiff to one that
 9 authorities could now obtain from the Defendants without Plaintiffs' knowledge. (CAC ¶¶ 665,
 10 666, 668.)

11 In sum, Plaintiffs have alleged that they experienced actual damage (including loss of
 12 value) and have stated facts sufficient at this stage for the Court to infer both additional actual
 13 damages as well as substantial interference with Plaintiffs' use and possession of their iDevice
 14 address books and iDevices.

15
 16 *d) Strict Products Liability*

17 Apple manufactured and sold iDevices to Plaintiffs. (CAC ¶ 686.) Apple co-
 18 manufactured and then sold or distributed Defendants' apps via its "App Store." (CAC ¶¶ 128,
 19 187-189.) However, Apple's iDevices had a serious design flaw that jeopardized Plaintiffs'
 20 privacy and Plaintiffs' property. In particular, Apple's design enabled the Defendant Apps to
 21 upload and acquire Plaintiffs' valuable and private personal data without their consent. (CAC ¶¶
 22 3, 61-63, 87, 107, 688, 699.)

23 As this caused Plaintiffs to suffer significant harm (their privacy was invaded, and
 24 property they kept on the iDevice was converted and transformed, CAC ¶ 695), Apple also failed
 25 to warn its consumers that it had not protected the iDevice contact database from security and
 26 privacy intrusions. The foregoing gives rise to Plaintiffs' strict liability claims under design
 27 defect and failure to warn theories. (CAC ¶¶ 685-705.)

1 The elements of strict liability based on a design defect are: (1) a defect in the design of a
 2 product; (2) causation; and (3) injury. Nelson v. Superior Court, 144 Cal. App. 4th 689, 695
 3 (2006).³² Similarly, manufacturers are strictly liable for injuries caused by their failure to warn
 4 of dangers known to the scientific community at the time they manufactured or distributed their
 5 product. Johnson v. American Standard, Inc., 43 Cal 4th 56, 64-65 (2008).

6 Significantly, Apple does not challenge Plaintiffs’ allegations that the iDevices were
 7 designed defectively or that Plaintiffs suffered harm. Rather, Apple denies that its defective
 8 design caused Plaintiffs’ injuries and contends it had no obligation to warn about that the other
 9 Defendants’ Apps would be invading their privacy and taking their address books. (Apple’s
 10 MTD at 33.)

11 According to Apple, the App Developers – not Apple – made the apps that invaded
 12 Plaintiffs’ privacy, acquired Plaintiffs’ property without permission and took (through their apps)
 13 Plaintiffs’ address books after Plaintiffs purchased the iDevices from Apple, not at the exact time
 14 of purchase. Id. Therefore, Apple contends third parties (the apps in question) caused Plaintiffs’
 15 injuries, not Apple, and argues it cannot be strictly liable for its design unless it “contributed
 16 substantially to the harm” inflicted on Plaintiffs or “participated substantially in creating a
 17 harmful combined usage of the products.” Id. (citing O’Neil v. Crane, 53 Cal. 4th 335, 361
 18 (2012)).

19 While this statement of the law is correct, it is also exactly what Plaintiffs allege Apple
 20 did. Unlike O’Neil, 53 Cal.4th at 352, which involved piping and component replacement parts,
 21 and in which the respective manufacturers had no involvement with the making or marketing of
 22 each others’ products, here, Apple and the App Developers worked closely together, and Apple
 23

24 ³² A product design in California may be defective under the consumer expectations test or
 25 the risk-benefit test. Under the consumer expectations test, a product is defective in design if the
 26 plaintiff proves the product fails to perform as safely as an ordinary consumer would expect
 27 when used in an intended or reasonably foreseeable manner. Barter v. Lull Engineering, 20 Cal.
 28 3d 413, 430-432 (1978). Alternatively, under the risk benefit test, a product is defective in
 design if the plaintiff proves that the product’s design proximately caused injury, and the
 defendant fails to prove that on balance, the benefits of the challenged design outweigh the risk
 of danger inherent in such design. Id. Plaintiffs’ CAC satisfies both tests. (CAC ¶¶ 685-697.)

1 actually co-manufactured the App and reviewed the App for functionality, security and privacy
 2 concerns. (CAC ¶¶ 128, 142,187-189,194, 201-202, 212-214.) More particularly, Apple
 3 supplied the App Defendants with development tools and code to make the apps function,
 4 provided them access to its developer program, marketed and distributed the Apps for its own
 5 financial gain, and digitally activated the Apps for use on its closed system. (CAC ¶¶ 134, 142,
 6 152, 181-182, 187-189, 190-192, 194, 201, 208, 212-214.) Thus, Plaintiffs have alleged that
 7 Apple's design, which enabled the Apps to take Plaintiffs' personal data and examine Plaintiffs'
 8 social networks and most intimate relationships, contributed substantially to the harm they
 9 suffered. And Apple created a harmful combined usage of the products. (Id.; see also CAC ¶¶
 10 685-697.) Without Apple's design, marketing and distribution, Defendants' violations of
 11 Plaintiffs' rights could not have occurred. Apple knew and intended for the Apps to function in
 12 this manner. (CAC ¶ 687.) And when the intended use of a product inevitably results in the
 13 harm, as happened here when the Apps took advantage of the design flaw to invade Plaintiffs'
 14 privacy and acquire Plaintiffs' personal data, the law is clear that the exceptions delineated in
 15 O'Neil apply and Apple may be strictly liable. See, e.g., Tellez Cordova v Campbell-
 16 Hausfeld/Scott Felzger Co., 129 Cal. App. 4th 577 (2004) (holding that manufacturer is liable for
 17 a defective design under products liability where, as here, it specifically designs the product to be
 18 used together with another product and the joint usage results in harm).

19 Here, Apple specifically designed and intended its iDevices to be used with apps and
 20 designed its iPhone in an unsecure manner, wherein apps could take Plaintiffs' personal data.
 21 Thus, the harm Plaintiffs suffered (invasions of privacy and loss of or conversion of separate
 22 property)³³ was not only inevitable, but arose from a use that Apple intended.

23 Apple's argument against Plaintiffs' strict liability failure to warn claim fails for the same
 24 two reasons. First, while O'Neil does recognize that it is generally true that a manufacturer is
 25 under no duty to warn about dangers arising *entirely* from another manufacturer's product even if
 26 it is foreseeable that the products will be used together, as discussed above, the dangers to
 27

28 ³³ (CAC ¶ 694.)

1 Plaintiffs did not come *entirely* from the apps. O’Neil, 53 Cal 4th at 361-62. Apple co-
 2 manufactured the apps, taught App Defendants how to take data, supplied code and digitally
 3 activated the app for use on its closed system – that it told its consumers was private and secure.
 4 (CAC ¶¶ 121-123, 187-189, 212-214.) Thus, the harm inflicted upon Plaintiffs was not entirely
 5 from the Apps. It also derived directly from Apple.

6 Second, O’Neil expressly acknowledges that there is a duty to warn about the risks
 7 associated with another manufacturer’s product if “the intended use of [the] product inevitably
 8 creates a hazardous situation.” O’Neil, 53 Cal.4th at 361. As described above, Plaintiffs have
 9 alleged that this occurred. The situation in Tellez-Cordova is analogous. There, power tools
 10 manufactured by defendants were specifically designed to used with abrasive disks, which led to
 11 lung disease from asbestos exposure. Tellez-Cordova, 129 Cal. 4th at 580. Like here, the power
 12 tools themselves did not harm the plaintiff on their own. But when used together with the
 13 abrasive disks, as both manufacturers intended, they did harm the users. Id. In that situation,
 14 where the combined usage of the products in the very manner intended posed a risk that the
 15 manufacturers knew or should have known existed, they were obligated to warn the consumer.
 16 Id. at 585.

17 Combined, the usage of the iDevice and the Defendants’ apps in the very manner both
 18 Apple and the App Defendants meant for the products to be used posed a hazardous situation to
 19 Plaintiffs, namely the systematic invasion of Plaintiffs’ privacy and the taking of their address
 20 books. Thus, Apple may be strictly liable for its failure to warn as well.

21
 22 *e) Negligence*

23 Plaintiffs’ negligence claim is also well pleaded. The elements of negligence are duty,
 24 and damages proximately caused by the breach. El Chico Corp. v. Poole, 732 S.W.2d 306, 311
 25 (Tex. 1987). It is well settled that once a party voluntarily assumes a duty, that the party must
 26 exercise reasonable care to fulfill it. Bolin v. Tenneco Oil Co., 373 S.W.2d 350 (Tex. 1963).
 27 Plaintiffs’ CAC alleges Apple assumed a duty – not based on hidden agreements, but based on
 28 public assertions and statements to protect users’ privacy from third party apps, malware, or

1 harmful code, and on industry standards they, and their competitors, created. (CAC ¶¶ 87, 92,
2 101-102, 121-123, 140.)

3 Apple has publicly represented that apps may not have hidden features that take users'
4 personal information without permission. (CAC ¶¶ 87-99.) Steve Jobs, Apple's then CEO,
5 publicly stated that the App Store would not distribute Apps that steal your private data (i.e.,
6 one's contacts). (CAC ¶¶ 92, 96.) And Apple's guidelines and agreements with App
7 Developers, which are hardly private, purport to preclude malware and the taking without
8 consent of address book contents. (CAC ¶ 104-105.) Combined with Apple's acknowledgement
9 that the address book data in Contacts is owned by the user, that Apps were sandboxed, and
10 malware prohibited, Apple clearly assumed a duty to protect its users' privacy that conflicts with
11 its purported disclaimer. (CAC ¶¶ 198-207, 209.) In fact, as alleged in the CAC, Apple
12 represented to the FCC that it engaged in a rigorous review process of all apps in order to protect
13 their consumers' privacy. (CAC ¶ 206.) It should not be permitted to represent to the
14 government it is protecting consumers' privacy by reviewing apps for privacy and then disclaim
15 that duty through a web-based privacy policy. Furthermore, Apple publically expressed that the
16 address book was protected from incursion, *i.e.* sandboxed, and that the address book was private
17 and owned by its user. (CAC ¶¶ 209, 213.)

18 As Plaintiffs alleged that Apple breached this duty and that the breach caused Plaintiffs to
19 suffer damage to their property (e.g., impaired performance, the need for inspection and repair,
20 use of data time, and theft of their property), Plaintiffs' negligence claim should not be
21 dismissed.

22 As far as whether Apple sufficiently disclaimed this duty, and its statements suggest
23 otherwise, this issue is not proper grounds for dismissal at this time. Not only are the documents
24 submitted by Apple outside the pleadings, Apple expressly assumed a duty to protect its users in
25 this fashion. The law is clear that a party may be liable for failure to protect someone from a
26 known harm and that a duty of reasonable care exists when reasonable men and women would
27 recognize it and agree that it exists. Otis Eng'g Corp. v. Clark, 668 S.W.2d 307, 310 (Tex.
28 1983); Missouri, K & T. RR. Co. of Texas v. Wood, 66 S.W. 449 (Tex. 1902). Here, the risks of

1 harm were known and foreseeable,. Apple knew and even participated in the wrongdoing. By
 2 knowingly failing to protect its customers from malware that takes personal data without a user's
 3 consent, Apple was negligent. See, e.g., Wilson v. Brister, 982 S.W.2d 42 (Tex. 1998).
 4 Moreover, Apple owed a duty to its customers to protect them from violations of their rights by
 5 third parties (the App Defendants), particularly when they have in whole or in part created the
 6 circumstances that led to the criminal conduct. Berly v. D & L Sec. Svcs. and Investigations,
 7 Inc., 876 S.W.2d 179, 188 (Tex. 1994). Thus, Apple's motion to dismiss Plaintiffs' negligence
 8 claim should be denied.

9 Significantly, this is nothing like the cases cited by Apple concerning the latent defects
 10 and retailers who do not know a product is defective. Here, Plaintiffs allege that Apple *knew*
 11 each App was defective and that Apple was, for example, told by scientists that Gowalla was
 12 engaging in address book theft. (CAC ¶¶ 216, 743.) Far from addressing the problem, as Apple
 13 claims it did, Apple ignored the complaint and continued to provide malicious, address book-
 14 stealing apps like Gowalla to unknowing consumers such as Plaintiffs.³⁴ (CAC ¶ 216.)
 15 Plaintiffs' negligence claim should not be denied.

16
 17 *f) Aiding and Abetting*

18 Apple's opposition to Plaintiffs' claim that Apple is liable for aiding and abetting the
 19 wrongdoing of the App Defendants again ignores the substance of Plaintiffs' allegations in favor
 20 of formalistic irrelevancies. First, it contends that aiding and abetting is not a stand-alone cause
 21 of action under California law. The fact that Plaintiffs' aiding and abetting allegations are set out
 22 in a separate claim merely provides clarity to the complaint by specifying that Plaintiffs contend
 23 that Apple is liable not just for its own actions but for those of the App Defendants. Second,
 24 Apple argues that Plaintiffs have not pled that Apple acted with knowledge of those acts. That
 25

26
 27 ³⁴ Based on these allegations, Apple would not even be entitled to the innocent retailer
 28 defense under Texas Civil Practices and Remedies Code § 82.003 because the pleadings allege
 that Apple knew that Defendants' apps were acquiring and uploading address book information
 without consumers' consent. (Id.)

1 simply ignores the complaint, which alleges, for example, that “[d]espite knowing that design
2 flaws left iDevices’ mobile address books insecure, Apple nevertheless helped the App
3 Defendants deploy malicious apps containing these same harmful features to Plaintiffs’ and
4 Class Members’ iDevices.” (CAC ¶ 142.) The complaint details Apple’s close involvement in
5 the development process, its tight app review process, and its awareness of the security flaw in
6 the devices it designed and sold. Plaintiffs’ claim against Apple based on its aiding and abetting
7 of the App Defendants is adequately pled.

8 **IV. CONCLUSION**

9 For the forgoing reasons, Plaintiffs respectfully request that the Court deny Apple’s
10 motion to dismiss.³⁵ To the extent the Court believes that the factual pleading is inadequate,
11 Plaintiffs request leave to amend.

12
13 DATED: December 2, 2013

KERR & WAGSTAFFE LLP

14
15 By: s/ Michael Ng
MICHAEL NG

16 Attorneys for *Opperman* Plaintiffs
17
18
19
20
21
22
23
24
25

26 _____
27 ³⁵ Plaintiffs believe the RICO claim is well plead. However, in light of Defendants’ clear
28 liability on the numerous other claims based on the same facts, Plaintiffs elect not to prosecute
that claim at this time and have no objection to its dismissal without prejudice as to these
Defendants.

Dated: December 2, 2013

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

By /s/ David M. Given
David M. Given
Nicholas A. Carlin
PHILLIPS, ERLEWINE & GIVEN LLP
50 California Street, 32nd Floor
San Francisco, CA 94111
Tel: 415-398-0900
Fax: 415-398-0911

By /s/ James M. Wagstaffe
James M. Wagstaffe
Michael K. Ng
Ivo M. Labar
Michael J. Von Loewenfeldt
KERR & WAGSTAFFE LLP
100 Spear Street, 18th Floor
San Francisco, CA 94105
Tel: 415-371-8500
Fax: 415-371-0500

Interim Co-Lead Counsel for Plaintiffs

Carl F. Schwenker (TBN 00788374,)
LAW OFFICES OF CARL F. SCHWENKER
The Haehnel Building
1101 East 11th Street
Austin, TX 78702
Tel: 512.480.8427
Fax: 512.857.1294
Email: cfslaw@swbell.net

Plaintiffs' Liaison Counsel

Jeff Edwards (TBN 24014406; *pro hac vice*)
EDWARDS LAW
The Haehnel Building
1101 East 11th Street
Austin, TX 78702
Telephone: 512.623.7727
Facsimile: 512.623.7729

Jennifer Sarnelli
James S. Notis
Gardy & Notis LLP
560 Sylvan Avenue
Englewood Cliffs, NJ 07632
Email: jsarnelli@gardylaw.com
jnotis@gardylaw.com

Plaintiffs' Steering Committee ("PSC")